HORIZON EUROPE PROGRAMME
HORIZON-CL3-2021-CS-01-01

A EUROPEAN CYBER RESILIENCE FRAMEWORK WITH ARTIFICIAL INTELLIGENCE -ASSISTED ORCHESTRATION & AUTOMATION FOR BUSINESS CONTINUITY, INCIDENT RESPONSE & INFORMATION EXCHANGE

D6.1: Interim report on Dissemination, Exploitation, Standardization & Sustainability

Abstract: This document represents the first interim report on activities performed by the PHOENIIX project on dissemination, exploitation, standardization & sustainability, within the first 18 months of the project. The plans and efforts described within this document, were undertaken as part of the Work Package 6 activities and specifically as part of Tasks 6.1 (as regards to Communication and Dissemination activities), Task 6.2 (as regards to Exploitation & Standardization activities) and Task 6.3 (as regards to Stakeholder engagement and liaisons with other activities).

This document is split into four different sections, each one corresponding to the different concepts of the title (i.e., dissemination, exploitation, standardization & sustainability).

Several key achievements of the consortium within this first period of the project are presented in this document, ranging from the communication and dissemination activities of the consortium such as scientific papers published, contributions to conferences and other events, activities on social media and traditional communication channels, to the efforts related to the contribution in existing standardization activities, the identification of exploitable assets and the first version of exploitation plans.

Contractual Date of Delivery	31/12/2023
Actual Date of Delivery	31/12/2023
Deliverable Security Class	PU

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No 101070586

Editor	*Chatzopoulou Argyro (APS)*
Contributors	Karras Apostolos (APS), Theodoropoulou Eleni (COSM), Limperopoulos George (COSM), Luna Eva Rodriguez (UPC), Marinos Tsantekidis (AEGIS), Ioannis Kakogiannos (WSE)
Quality Assurance	*Alejandro Quintanar (SEA)* *Rodrigo Diaz (ATOS)*

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No 101070586

Document Revisions & Quality Assurance

Internal Reviewers

Reviewer #1: #11 ATOS IT SOLUTIONS AND SERVICES IBERIA SL (ATOS)

Reviewer #2: #9 SOCIAL ENGINEERING ACADEMY (SEA) GMBH (SEA),

Revisions

Version	Date	By	Overview
0.1	05/09/2023	APS	Document template: ToC
0.2	1/11/2023	APS	First integration of section 3
0.3	5/11/2023	COSM	First integration of section 3
0.4	15/11/2023	UPC	First integration of section 2
0.5	31/11/2023	APS	First integration of section 4
0.6	7/12/2023	UPC	Updated Section 2
0.7	08/12/2023	COSM	Updated Section 5
0.8	09/12/2023	APS, WSE	Updated Sections 3, 4. Added closing remarks
0.9	22/12/2023	ATOS	Quality Review
0.9	27/12/2023	SEA	Quality Review
1.0	28/12/2023	APS	Final version

Contents

1 Introduction

PHOENI2X aims to design, develop, and deliver a Cyber Resilience Framework providing Artificial Intelligence (AI) - assisted orchestration, automation & response capabilities for business continuity and recovery, incident response and information exchange, tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity. Through the deployment PHOENI2X Cyber Resilience Centres (PHOENI2X CRCs), OES will gain:

(i) enhanced Situational Awareness with AI-assisted Prediction, Prevention, Detection & Response capabilities, and business risk impact assessment-based prioritisation;

(ii) proactive and reactive Resilience Automation, Orchestration, and Response (ROAR) mechanisms, providing Business Continuity, Recover and Cyber & Physical Incident Response;

(iii) increased Preparedness through relevant Serious Games and realistic Resilience Cyber Range (RCR) Assessment & Training;

(iv) timely and actionable Information Exchange between OES, National Authorities and EU actors, leveraging interoperable and standardised alerting and reporting mechanisms and processes.

To effectively achieve these goals, it is critical that planned activities take place that will ensure the:

- communication of the project activities and results,
- integration of standardized practices within the project development lifecycle,
- provision of feedback and added value to the relevant audiences,
- exploitation of the key exploitable results of the project and
- achievement of the sustainability of the solution.

The planning and activities to achieve the above are included within the tasks and activities prescribed in Work Package 6.

Specifically, work package 6 contains the following tasks:

Task 6.1: Communication & Dissemination Activities.

This task focuses on refining and executing the communication and dissemination plan of PHOENI2X. The associated activities will be planned and monitored through periodic monitoring reports and plan updates, which will also document refinements to the communication and dissemination plan (project and partner-specific), as needed.

Task 6.2 - Impact creation, Exploitation & Standardisation activities.

This task aims to facilitate the sustainability and impact of PHOENI2X. The task will investigate the market prospects for the project's outputs in the short and long term (i.e., 1, 3 and 5 years after the project), developing a detailed business plan and marketing strategy (later integrating results from the holistic T5.4 assessment – e.g., related to cost-effectiveness or. the regulatory compliance impact of the technologies and their adoption potential). It will also and deliver a report on the exploitation activities carried out within the project's duration. This task will also identify and evaluate the PHOENI2X IPR production and potentials. Moreover, the task will continuously investigate opportunities for PHOENI2X to contribute to relevant

cybersecurity standards and interoperability specifications, as well as to policymaking initiatives in areas of interest to the project (e.g., extensions to the Cyber Blueprint, Resilience Act, creation of Joint Cyber Unit).

Task 6.3 - Stakeholder Engagement and EC Initiatives' Liaisons.

This task focuses on the engagement of entities that could potentially adopt PHOENI2X (e.g., OES, National Authorities, private and public SOCs), as well as other EU cybersecurity stakeholders (ENISA, CSIRTs network, CERT-EU, Europol, ISACs) and policy makers who can provide valuable feedback but also promote the wider adoption of the PHOENI2X approach.

This document is structured to follow the key subjects detailed above. Specifically,

Section 2. Dissemination, describes the plans, efforts and results related to communication and dissemination of project information, results and activities.

Section 3. Exploitation, describes the plans, efforts and results related to the exploitation of the project key exploitable results.

Section 4. Standardization, describes the plans, efforts and results related to standardization.

Section 5. Sustainability and third-party interactions, describes the plans, efforts and results related to the sustainability of the project outcomes and the activities in relation to related external stakeholders.

Section 6. Closing remarks and future steps.

2 DISSEMINATION

2.1 Objectives of Task 6.1. on dissemination and communication

This task aims to refine and execute the communication and dissemination plan of the PHOEN2X project, which will use heterogeneous channels for its dissemination and communication activities. These activities will leverage electronic (online) channels, non-electronic (traditional) channels, as well as highly interactive and impactful dissemination channels such as social media. Dissemination and communication activities will be updated to follow the developments in the project. The consortium, in the grant agreement, has already defined the main activities through which the project and its results will be communicated to broader audiences, also disseminating the results to experts, related stakeholders, scientific communities in AI, and other pertinent domains, while additional interdisciplinary actions will be coordinated for bringing together the different communities, demonstrating their interactions and highlighting PHOENi2X potential for their respective needs. The associated activities will be planned and monitored through periodic monitoring reports and plan updates.

This chapter presents the PHOENI2X dissemination and communication strategy, the specific communication and dissemination activities carried out during the first 18 months of the project, and their impact which is measured through the related performance indicators.

2.2 Dissemination and Communication Strategy

PHOENI2X dissemination and communication strategy aims to promote, communicate and disseminate the activities and results of the project to the different stakeholders, based on the strategy included in the grant agreement and updated to follow the developments of the project.

Dissemination and communication are focused on making the project visible, creating understanding of the project and promoting participation in the project results. Therefore, the strategy needs to address the following aspects:

1. Objectives: aim of the dissemination.
2. Outcomes: what will be disseminated.
3. Target groups: who is the audience.
4. Resources: what medium will be used.
5. Timing: when it will be disseminated.

These different aspects have to be jointly addressed, to ensure effective communication and dissemination, for example that different target groups will be approached by different media, or that some results of the project will only be published in the last stage of the project. Then, communication and dissemination activities have to be updated according to the above mentioned issues and their impact and success measured with specific metrics as proposed in the grant agreement.

The dissemination and communication strategic approach is meant to be a dynamic. To this end, the consortium will constantly refine the strategy, according to the progress of the project, to focus on efficiently promoting the results at each stage and on progressively building buzz around the PHOENI2X offering. This way, communication and dissemination activities will be conceptually divided in four phases (see Figure 1):

1. Phase I - Planning: Definition of the Communication and Dissemination Plan. Generate visibility of the project by being shared, read, and seen on social media and website as well as on traditional media. Define Channels and formats: logo, visual identity, website, social media, etc.
2. Phase II – Implementation: Generate brand and Project awareness. The brand has to be recognized by stakeholders and potential customers. Generate interactions with stakeholders

and potential customers. Use blogs, articles, newsletters, press releases, events, etc., to engage with them. Update of the dissemination and communication plan. Dissemination of the first results of the project.

3. Phase III – Final Evaluation: Enhancement of the PHOENI2X visibility. Extensive public communication of the project and results. Dissemination of the results of the project.
4. Phase IV – Sustainability: Communication of impact and benefits of the project. Knowledge transfer.

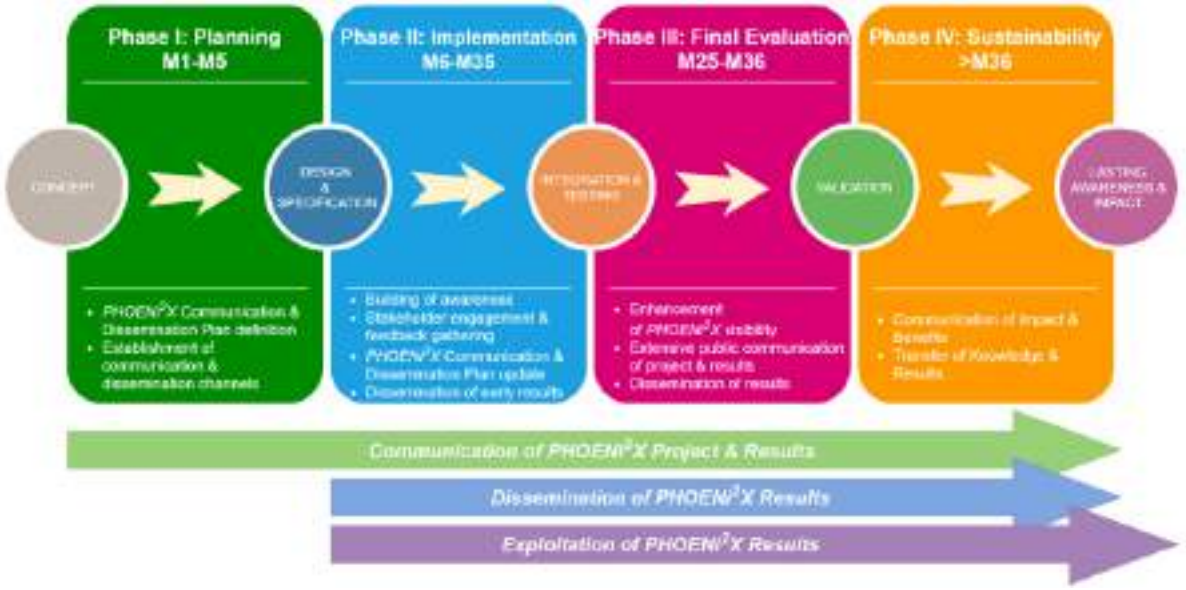


Figure 1: Communication, Dissemination and Exploitation Methodologies

The PHOENI2X project is addressing a broad range of recipients (target groups) including supply chain stakeholders, cybersecurity experts, IT organisations, research centres, public administrations, among others. To undertake an efficient communication and dissemination, it is crucial to have a good understanding of these target audiences to apply the appropriate customisation of the promotional material. Furthermore, each group has different needs and hence requires consequently a different approach.

The consortium will ensure that the elaborated promotional materials are appropriately adapted to the target audiences so that all activities can be tailored to the target groups' special information need. Table 1 shows that where initially identified as target groups of the PHOENI2X project:

Table 1 PHOENI2X target groups

Communities	**Key PHOENI2X Benefits**	**Group Interest & Related Impact**
Sci. & Tech. Community, Academics, Researchers	- Unified integration of existing knowledge on real-world designs - State-of-the-art progression	- Consideration of previous initiatives within PHOENI2X deployment - Knowledge exchange and tool utilization in additional research
General public, OES	- Explainable AI penetration for OES - Tangible advancement and resilience in OES services	- Strengthened AI-driven diagnostics with evidence-based justification

	- Improved resource and cost management	- Improved OES business operation - Impact in critical infrastructures' administration & operators' readiness
Policy makers, National/MS and EU authorities	- Validation, unification, and extension of existing security and resilience guidelines - Interdisciplinary coordination towards improved approaches	- Communication of outcomes in international initiatives and alliances - Current standard refinement and extension, promoting reliable penetration
SMEs & Industry	- Novel products, exploiting & promoting new technologies - Evaluation / reformation of existing practices	- Exploitation of PHOENI2X outputs for accelerating associated products and services within the various OES domains and AI

The information contained in Table 1 PHOENI2X target groups identifies some crude groups in order to create the different options regarding dissemination and communication. As part of the activities of Task 6.3., an analysis was carried out to further elaborate on these groups and propose further and more targeted engagement strategies and approaches. More information on this can be found in Section 5.STAKEHOLDER ENGAGEMENT AND LIAISON ACTIVITIES of this document.

2.3 Dissemination and Communication Plan

The objective of this section is to describe the specific plan for PHOENI2X project dissemination and communication activities defined at the beginning of the project. This plan will be carried out throughout the project lifetime so that the expected results will be communicated as widely and effectively as possible. These activities include participation in events/conferences/workshops, preparation of scientific papers, articles and other generic publications, foster relationships and synergies with related projects, among others.

Thorough all the project duration, it is expected that PHOENI2X will be present in international events and conferences. The following categories of events will be considered:

- Journal publications, international conferences and special issues.
- Workshops: especially those organized by related H2020 projects. PHOENI2X will actively seek communication and exchange with related R&D EU Projects. Particularly the parallel projects under the same H2020 call and topic are likely to be relevant.
- EU focused events: PHOENI2X members will actively participate in the activities organized by the EC, related to the cyber-security and business continuity fields. PHOENI2X aims at receiving the latest information about other H2020 programme projects and implementations, standards, and regulatory activities.
- Meetings with key stakeholders.
- Collaboration with other EU projects and Policy Makers

PHOENI2X will periodically publish the project results through the Blog, Newsletters and Press Releases to reach all the target audiences previously identified. To this end a plan has been elaborated for the Blog entries, Newsletters and Press Releases, as detailed in next sections.

2.3.1 Blog entries plan

Blog posts in PHOENI2X are published on a monthly basis and are produced by all partners with the view to communicate project findings as well as ignite interesting conversations. These blogs are available in the project website (https://phoeni2x.eu/blog/).

The first entry has been generated by the technical coordinator and provides an overview of the PHOENI2X framework. By the end of the project blogs entries will be focused on the use cases deployment and integration results. Table 2 below depicts the plan for the blog production.

Table 2 PHOENI2X Blog entries calendar

	Blog entries calendar				
#	**Months/Year**	**Partner**	**#**	**Months/Year**	**Partner**
1	October 2022	SANL	18	March 2024	COSM
2	November 2022	UPAT	19	April 2024	UPAT
3	December 2022	ATOS	20	May 2024	WOS
4	January 2023	SEA	21	June 2024	SEA
5	February 2023	WOS	22	July 2024	EUNL
6	March 2023	AEGIS	23	August 2024	SANL
7	April 2023	UiO	24	September 2024	ATOS
8	May 2023	NCSA	25	October 2024	UiO
9	June 2023	UPC	26	November 2024	NPS
10	July 2023	NPS	27	December 2024	NCSA
11	August 2023	DSA	28	January 2025	AEGIS
12	September 2023	SANL	29	February 2025	UPC
13	October 2023	EUNL	30	March 2025	DSA
14	November 2023	AEGIS	31	April 2025	APS
15	December 2023	APS	32	May 2025	COSM
16	January 2024	PPC	33	June 2025	PPC
17	February 2024	FGC			

2.3.2 Newsletters / Press release plan

Newsletters and Press Releases PHOENI2X will be published periodically in the PHOENI2X web, under News and Events (https://phoeni2x.eu/news-events/).

The PHOENI2X newsletter offers the appropriate means to carry out direct proactive communications to the targeted stakeholders, the European Commission, researchers and potential interested investors. The newsletter will be released at every key stage of the project.

PHOENI2X press releases will disseminate the project by informing about the real benefits that PHOENI2X can offer to the stakeholders' groups identified in Table 1. It is planned that three of the Press Releases will be published by the Use Case owners of the project, in national magazines and/or newspapers of the partner country. Table 3 below depicts the plan for the Newsletters and Press Releases production.

Table 3 PHOENI2X Newsletters and Press Releases calendar

	Newsletters calendar		**Press Releases calendar**
#	**Months/Year**	**#**	**Months/Year**
1	February 2023	18	February 2023

2	July 2023
3	November 2023
4	March 2024
5	July 2024
6	November 2024
7	March 2025
8	June 2025

19	July 2023
20	December 2023
21	March 2024
22	July 2024
23	November 2024
24	March 2025
25	June 2025

2.3.3 Methodology for evaluation

Dissemination and Communication Activities of the project will be monitored and coordinated by the task leader. Performance indicators have been defined to measure the impact of the conducted activities and to be able to adjust the dissemination and communication strategy for achieving the expected outcomes and maximizing visibility. Such metrics will allow having a constant view of the quantitative amount and the qualitative effectiveness of the dissemination and communication activities conducted.

In the grant agreement, the consortium established several performance indicators about communication and dissemination (see Table 4), for the whole duration of the project.

Table 4 PHOENI2X Dissemination and Communication Activities: KPIs and Targets in the grant agreement

Channels	**Target Audience**	**Activity/Measures**	**Measurable indicators and target value**
Scientific publications	S&T community, Researchers, Academics	Journal publications	≥8 peer-reviewed publications
		International conferences	≥15 peer-reviewed publications
		Special issues	≥ 5 special issues/book chapters
International events	S&T community, Industry, OES	Workshops/Special sessions	≥2 workshops/special sessions; ≥40 attendees
Demonstrators	Policy makers	EU-focused event	≥1 demonstration
		Technical, Academic, Industrial events	≥3 demonstrations, webinars & training events
Networking/ Outreach	Academics, Researchers, Industry	Interactive face-to-face networking	≥4 interactive face-to-face networking EU event
	Research peers	Collaboration with other projects	≥4 synergies established with pertinent EU project
	Policy makers	Collaboration with Policy Makers	≥1 meeting with OES stakeholders per UC country; ≥2 meetings with cybersecurity policy makers at national and EU level
Electronic activities	General Public	Project website	Deployed in M2; ≥1.000 accesses annually; ≥100 downloads (deliverables, results & materials)
		Video clips	≥ 2 online video clips; ≥ 1000 views
		Social media	2 project accounts in Facebook and Twitter;

			≥100 connections/followers on each; ≥30 posts per year
	Industry, OES operators	Press releases/ newsletters	≥8 press releases; ≥8 newsletters
	Academics	S&T communities / research networks	2 project accounts in ResearchGate, LinkedIn; ≥100 connections/followers on each; ≥30 posts per year
Nonelectronic activities	Industry, OES, Policy makers	Presentation material	≥8 flyers/brochures, ≥3 posters, ≥2k hard copies
	General Public	Traditional media	≥1 articles/interviews to national magazines &/or newspapers per participating country

To ensure the success of the dissemination and communication activities in Task 6.1, a plan has been established for monitoring the performance indicators, as listed in Table 5 and Table 6.

Table 5 PHOENI2X Dissemination Plan - KPIs

Activity/Measures	**Targets**			**Expected Impact**
	Y1	**Y2**	**Y3**	
Journal publications	2	2	4	Validation of the project findings and results. Promotion of the results to scientific communities. Exchange of knowledge with relevant communities and initiatives.
International conferences	2	6	7	
Special issues	-	2	3	
Workshops/Special sessions	1	1	1	Increased collaboration with other initiatives and projects for joint research, information exchange and dissemination. Liaisons. Validation of project's concept, findings and progress.
Collaboration with other projects	1	1	2	
EU-focused event	-	-	1	Knowledge exchange with relevant communities and initiatives. Promotion of results to relevant communities and initiatives.
Technical, Academic, Industrial events	1	1	1	
Interactive face-to-face networking	-	1	3	Contact to external stakeholders to promote PHOENI2X solutions. Increased awareness.
Collaboration OES stakeholders	-	-	1	
Collaboration with cybersecurity policy makers	-	1	1	

Table 6 PHOENI2X Communication Plan - KPIs

Activity/Measures	Targets			Expected Impact
	Y1	Y2	Y3	
Project website accesses	1000	1000	1000	Main online information channel. Communication of project news, events and results. Increased awareness.
Downloads	100	100	100	
Blog posts	9	12	12	
Social media Twitter Followers Posts	 50 30	 75 30	 100 30	Attainment of interest of stakeholders active in social media. Sharing knowledge with other projects and initiatives. Drive engagement with the project.
LinkedIn Connections Posts	 100 30	 150 30	 200 30	
Facebook Followers Posts	35 30	50 30	100 30	Attainment of interest of general public active in social media. Drive engagement with the project.
Video clips	-	1	1	
Press releases	2	3	3	Promotion of results to relevant communities and initiatives. Proactive communications to the targeted stakeholders, the European Commission, researchers.
Newsletters	2	3	3	
Flyers/ Brochures	2	3	3	Promotion of the project to stakeholders and scientific community. Attainment of interest. Drive engagement with the project.
Posters	1	1	1	
General Public	-	1	2	Attainment of interest of general public. Drive engagement with the project.

2.4 Dissemination and communication activities

In this section, the specific communication and dissemination activities carried out during the first 18 months of the project are described. These activities include, but are not limited to, the participation in events/conferences/workshops, preparation of scientific papers, articles and other general publications, blog entries, newsletters and press releases, and fostering relationships and synergies with related projects. In addition, the KPIs related to communication and dissemination are reviewed.

2.4.1 PHOENI2X workshops

During the first 18 months of the project, PHOENI2X has organized and sponsored two workshops.

CyberHunt 2022: On December 17, 2022, PHOENI2X co-sponsored the 5th Workshop on Cyber Threat Intelligence and Hunting (CyberHunt2022[1]) organized by the Digital Security Group of the University of Oslo, a partner in PHOENI2X, in conjunction with the 2022 IEEE International Conference on Big Data (IEEE BigData 2022[2]). The main focus of the workshop was to provide a forum for experts from academia, industry and government to discuss advances on the domain of CTI and other related domains that rely on and make use of CTI. Two partners from the PHOENI2X, SANL and UiO,

[1] https://cyberhunt2022.cyberhunt.no/
[2] https://bigdataieee.org/BigData2022/

participated in the workshop (see Figure 2). Konstantinos Fysarakis from Sphynx Analytics, serving as the PHOENI2X technical coordinator, gave a keynote highlighting challenges tackled by PHOENI2X ("Towards Integrated and Adaptive Cybersecurity Operations with Cross-Border Collaboration – A European Perspective"), as well as presented "A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness" (a PHOENI2X -related scientific paper, co-authored by Sphynx Analytics, University of Oslo & the Technical University of Crete).

Figure 2: CyberHunt2022 Workshop

IOSEC 2023: On April 20, 2023, PHOENI2X co-organized the 4th International workshop on Information & Operational Technology (IT & OT) security (IOSEC 2023[3]) held in Vilanova i la Geltrú, in conjunction with the 19th International Conference on the Design of Reliable Communication Networks (DRCN2023[4]). The workshop has been organized jointly with the EU-funded projects, JCOP[5], IntellIoT[6], and FISHY[7]. The workshop brought together more than 40 experts from cybersecurity and Artificial Intelligence fields, to discuss security problems and solutions for advancing the collective science and practice of IT and OT security. Figure 3 sketches the program of the workshop.

Figure 3: IOSEC2023 Workshop

[3] https://drcn2023.upc.edu/IOSEC2023.html
[4] https://drcn2023.upc.edu/
[5] https://jcop.eu/
[6] https://intelliot.eu/
[7] https://fishy-project.eu/

Two PHOENI2X partners, AEGIS and UPC, attended the IOSEC 2023 Workshop within the DRCN2023 conference co-organized by the PHOENI2X project.

CyberHunt 2023: On December 17, 2023, PHOENI2X co-sponsored the 6th Workshop on Cyber Threat Intelligence and Hunting (CyberHunt2023[8]) in conjunction with the 2023 IEEE International Conference on Big Data (IEEE BigData 2023[9]) in Sorrento, Italy. This workshop brought together experts from academia, industry, and government to discuss advances on the domain of Cyber Threat Intelligence. Three partners from the project, AEGIS, UiO, and UPAT, attended the workshop presenting two PHOENI2X related scientific papers: "AMINet: An Industrial Honeynet for AMI Systems" co-authored by UPAT and PPC; and "Enhancing Cyber Threat Hunting: A Visual Approach with the Forensic Visualization Toolkit" authored by AEGIS.

Figure 4: CyberHunt 2023 Workshop

[8] https://cyberhunt2023.cyberhunt.no/
[9] https://bigdataieee.org/BigData2023/index.html

2.4.2 Participation in Events/conferences/fairs

PHOENI2X project has co-sponsored the CyberHOT[10] 2022 and CyberHOT 2023 Summer Schools.

CyberHOT 2022: On September, 29 and 30, 2022, the Cybersecurity Hands-On-Training (CyberHOT) Summer School was organized in Chania, Crete under the auspices of NATO Maritime Interdiction Operational Training Center(NMIOTC). PHOENI2X project was one of the sponsors and PhD students from PHOENI2X consortium (see Figure 4) participated in the event that joint around 100 participants from different European countries.

The CyberHOT Summer School has been jointly sponsored by the EU funded projects: PHOENI2X, CyberSecPro[11], SENTINEL[12], CYRENE[13], InteliIoT[14], EnerMan[15], SecOPERA[16], JCOP, REWIRE[17] and EDGELES[18].

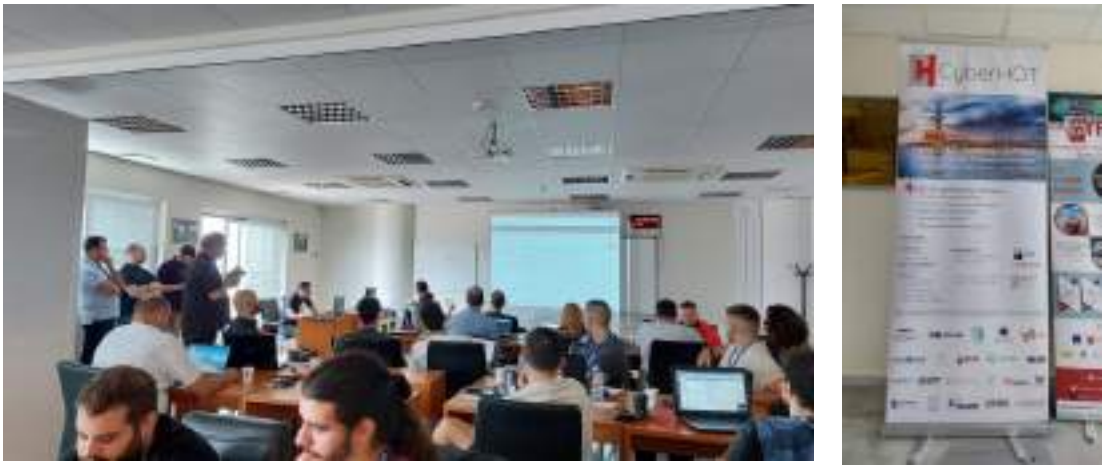


Figure 4: CyberHOT 2022

CyberHOT 2023: PHOENI2X has co-sponsored the Cybersecurity Hands-On-Training (CyberHOT) Summer School organized in Chania, Crete. The CyberHOT Summer school joined around 100 participants from different European countries which participated in several sessions addressing the research of vulnerabilities of known components, the exploitation of existing vulnerabilities and privilege elevation on compromised targets. The work conducted in the PHOENI2X was presented in the summer school (see Figure 5).

[10] https://www.cyberhot.eu/
[11] https://www.cybersecpro-project.eu/
[12] https://sentinel-project.eu/
[13] https://www.cyrene.eu/
[14] https://intelliot.eu/
[15] https://enerman-h2020.eu/
[16] https://secopera.eu/
[17] https://rewireproject.eu/
[18] https://edgeless-project.eu/

Figure 5: CyberHOT 2023

PHOENI2X partners participated the following events on behalf of the PHOENI2X project, apart from the CyberHunt 2022 and IOSEC 2023 workshops previously presented.

DRCN 2023 Panel: On April 18, 2023, PHOENI2X and FISHY EU-funded project sponsored the panel "Reliability, are you for real?" with the DRCN2023 conference (see Figure 6). Two PHOENI2X partners participated in the panel, Rodrigo Díaz (ATOS) and Xavi Masip (UPC), and the other participants were Oscar Carrasco (Casa-systems), Dominique Verchere (NOKIA Bell Labs), Matthias Gunkel (DT), Admela Jukan (TUBS) and Dominic Schupke (Airbus).

Figure 6: DRCN Panel - Reliability, are you for real?

Navigating standards and overcoming bottlenecks for SME growth[19]: STAND4EU and HSbooster.eu has co-organized an online Workshop entitled "Navigating standards and overcoming bottlenecks for SME growth", see Figure 7. The workshop took place on Wednesday 15 November, from 10:30 am to 12 pm CET. During the interactive workshop, the obstacles identified by STAND4EU in the interplay between research, innovation and standardisation were presented and the participants were allowed to contribute to shaping recommendations on how to make the standards development process more efficient. This event is part of the Meeting Standards campaign organised by Small Business Standards

[19] http://stand4eu.eu/assets/docs/2023-11-15%20Programme%20-%20MS%20STAND4EU-HSbooster%20Workshop%20-%20Meeting%20Standards%20-%20Final.pdf

to raise awareness of the importance of standardisation and facilitate knowledge sharing among SMEs. The event was attended by the partner APS.

Figure 7: Navigating standards and overcoming bottlenecks for SME growth Workshop

Infocom World 2023[20]/ Scientific Session: "Modern Research and Development Projects: Creating the Pillar for Investment and Innovations in the ICT Converged (Vertical) Markets": On December 14, 2023, the PHOENI2X project was presented by George Daniil in the scientific session organised by OTE (mother company of COSMOTE). The conference hosted 25 EU-funded R&D projects, while the PHOENI2X project was included in the 8th session dedicated to "AI for the Support of Cyber Resilience and (Cyber-) Security in Modern 5G/B5G Infrastructures", along with CyberSecDome (https://www.linkedin.com/posts/cybersecdome-eu-project_cybersecdome-ai-cybersecurity-activity-7112142742545178624-DenW/), REWIRE (https://rewireproject.eu/) and TRACY (https://www.tracy-project.eu/) projects.

IEEE CSCN 2023 conference[21]: On November 6, 2023, a PHOENI2X project related paper was presented by Marinos Tsantekidis on behalf of Alexis Lekidis, at the IEEE Conference on Standards for Communications and Networking (CSCN), co-located with the one6G Summit 2023 (see Figure 8).

Figure 8: IEEE CSCN 2023 conference

[20] https://infocomworld.gr/
[21] https://cscn2023.ieee-cscn.org/

The paper entitled "Risk assessment method for 5G-oriented DLMS/COSEM Communications" proposed a risk assessment method, developed in the PHOENI2X energy use case, based on the NIST SP 800-30 standard, for identifying vulnerabilities, as well as to classify them according to a risk matrix based also on their impact on the AMI system.

IEEE CSR 2023 Conference[22]: On July 31, 2023, the PHOENI2X project related paper *"Reviewing BPMN as a Modeling Notation for CACAO Security Playbooks"* was presented by M. Zych, from UiO, in the IEEE International Conference on Cyber Security and Resilience (CSR) conference.

ISBeRG Railways Biannual Meeting: During the week of the 6th of November, the ISBeRG[23] Railways Biannual Meeting was held on FGC premises, in Barcelona. ISBERG is an International Suburban Rail Benchmarking Consortium, see Figure 9, led by the Imperial College of London, and consisting of 15 suburban rail operators, coming from Copenhagen, Cape Town, Hong Kong, Barcelona, London, Melbourne, Munich, New York, Oslo, San Francisco and Sao Paulo. This program monitors and evaluates the efficiency of the operators using various Key Performance Indicators. One of the sessions was dedicated to innovation, where Carles Miralpeix i Llorach, a member of FGC, presented the current situation of the enterprise in terms of innovation, focusing on the main projects in which FGC is participating. In this presentation, he explained the importance of projects such as PHOENI2X to improve railway cybersecurity, one of the main pillars of the industry as a critical infrastructure and service.

Figure 9: ISBeRG - International Suburban Rail Benchmarking Group

Cybersecurity, AI and quantum computing, will we ever be in a safe environment? session of the Equity and Artificial Intelligence Research Coffee[24]**:** PHOENI2X Project has been presented by Xavi Masip from UPC, in the "Cybersecurity, AI and quantum computing, will we ever be in a safe environment?" session of the "Equity and Artificial Intelligence Research Coffee" held the 21st November 2023 in the Universitat Politècnica de Catalunya (UPC). In the session, see Figure 10, the role of AI in threats detection and prevention, as well as the PHOENI2X approach used for critical infrastructures, mainly energy, transport and health, were discussed.

[22] https://www.ieee-csr.org/
[23] https://www.isberg-web.org/
[24] https://bibliotecnica.upc.edu/investigadors/research-cafe

Figure 10: Equity and Artificial Intelligence Research Coffee

2.4.3 Publications

2.4.3.1 Journals

During the first 18 months of the project two journal papers have been published.

- ***A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things***, Rodríguez, E., Otero, B., Canal, R. (2023). Sensors, 23(3), 1252, DOI: https://doi.org/10.3390/s23031252. Open access. (JCR 3.9 Q2)

  Abstract: Recent advances in hardware and information technology have accelerated the proliferation of smart and interconnected devices facilitating the rapid development of the Internet of Things (IoT). IoT applications and services are widely adopted in environments such as smart cities, smart industry, autonomous vehicles, and eHealth. As such, IoT devices are ubiquitously connected, transferring sensitive and personal data without requiring human interaction. Consequently, it is crucial to preserve data privacy. This paper presents a comprehensive survey of recent Machine Learning (ML)- and Deep Learning (DL)-based solutions for privacy in IoT. First, we present an in depth analysis of current privacy threats and attacks. Then, for each ML architecture proposed, we present the implementations, details, and the published results. Finally, we identify the most effective solutions for the different threats and attacks.

- ***Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework,*** Jullian, O., Otero, B., Rodriguez, E., Gutierrez, N., Antona, H., & Canal, R. (2023). Journal of Network and Systems Management, 31(2), 33, DOI: https://doi.org/10.1007/s10922-023-09722-7. Open access. (JCR 3.6 Q3)

  Abstract: The widespread use of smart devices and the numerous security weaknesses of networks has dramatically increased the number of cyber-attacks in the internet of things (IoT). Detecting and classifying malicious traffic is key to ensure the security of those systems. This paper implements a distributed framework based on deep learning (DL) to prevent many different sources of vulnerability at once, all under the same protection system. Two different DL models are evaluated: feed forward neural network and long short-term memory. The models are evaluated with two different datasets (i.e.NSL-KDD and BoT-IoT) in terms of performance and identification of different kinds of attacks. The results demonstrate that the

proposed distributed framework is effective in the detection of several types of cyber-attacks, achieving an accuracy up to 99.95% across the different setups.

2.4.3.2 Conferences

During the first 18 months of the project eight papers have been published in International conferences.

- ***Cyber-security measures for protecting EPES systems in the 5G area***. Lekidis, A. (2022). In 17th International Conference on Availability, Reliability and Security (ARES '22), DOI: https://doi.org/10.1145/3538969.3544476.
  Abstract: The recent technological advance in the fifth generation of telecommunication networks (5G) has led to a evolutions in many domains, including connected cars, manufacturing and electricity. A technological domain that had large benefits from this advance is the Electrical Power and Energy System (EPES). Despite the simplicity and efficiency that 5G brings there are also underlying risks that are slowing down its adoption. These risks are caused by the presence of convergence connectivity interfaces in legacy infrastructures that were built with no security in mind. Specifically, EPES systems are often targeted by cyber criminals to cause massive blackouts in entire cities or countries that in turn lead to societal impact, such as consumer discomfort. In this work we propose a cyber-security measures for 1) early-stage detection of cyber-security incidents and 2) protecting against them through applicable security measures. The proposed measures are applied to a Hydroelectric Power Plant (HPP) of the Public Power Corporation (PPC). The cyber-attacks are performed in a 5G-enabled smart meter that measures power production and transmits measurements to PPC's control center through the use of 5G Network Function Virtualization (NFV) technologies, such as network slicing. To protect against the attacks, cyber-security measures are applied and incorporated in a cyber-security platform, that was developed within the PHOENIX H2020 project. The measures are used to detect the attacks and perform necessary mitigation actions for restoring the HPP operation.
- ***A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness***. Fysarakis, K., Mavroeidis, V., Athanatos, M., Spanoudakis, G., & Ioannidis, S. (2022). In IEEE International Conference on Big Data (Big Data), DOI: 10.1109/BigData55660.2022.10020736.
  Abstract: With digital technologies now being part of the fabric of our societies, identifying and managing cybersecurity threats becomes imperative. Within the European Union, several initiatives are underway, aiming to motivate, regulate and eventually orchestrate the establishment of capacity and enhancement of situational awareness, incident response, and preparedness capabilities, with an expected emphasis on operators of essential services and state actors entrusted with cybersecurity. In this context, the institution of cooperation and information exchange channels to allow for coordinated cross-border responses to large-scale incidents is particularly prioritized. Motivated by the above, this work presents a conceptual blueprint in support of architecting and establishing interoperable Cyber Security Operations Centres that combine capacity for situational awareness, incident response, and preparedness, also benefiting from the interplay between them, ultimately enhancing national cybersecurity capabilities, cross-border collaboration, and national supervision of their critical sectors, in line with current and upcoming regulatory requirements and the ever-increasing need for national and international cooperation.
- ***Risk Assessment Method for 5G-oriented DLMS/COSEM Communications***. Lekidis, A. (2022). In IEEE Conference on Standards for Communications and Networking (CSCN).

Abstract: The Advanced Metering Infrastructure (AMI) is lately introduced to ensure the real-time exchange of smart meter measurements and their availability for both utilities as well as their customers. DLMS/COSEM is the mostly used protocol for AMI system as well as allows the integration in 5G-enabled network slices to increase the reliability of energy measurement exchange and availability of sufficient data to calculate energy demand. Nevertheless, such integration augments the threat landscape and increases the probability of cyber-attacks by malicious entities, which aim at the exploitation of vulnerabilities. In this paper, we propose a risk assessment method based on the NIST SP 800-30 standard, for identifying such vulnerabilities as well as to classify them according to a risk matrix based also on their impact on the AMI system. The method is then applied to the DLMS/COSEM, in order to identify its vulnerabilities, which may be later be exploited within a cyber-attack aiming in disruption the AMI system operation. Moreover, it is demonstrated through a 5G-enabled emulated smart home network which is used to exploit smart meter vulnerabilities and then through a lateral movement to conduct attacks causing fluctuations on PhotoVoltaic (PV) systems and energy storage batteries.

- ***PHOENI²X–A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange***. Fysarakis, K., Lekidis, A., Mavroeidis, V., Lampropoulos, K., Lyberopoulos, G., Vidal, I. G. M. (2023). In 2023 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2023), DOI: 10.1109/CSR57506.2023.10224995.

  Abstract: As digital technologies become more pervasive in society and the economy, cyber-security incidents become more frequent, but also more impactful. Based on the NIS & NIS2 Directives, EU Member States and their Operators of Essential Services (OES) must establish a minimum baseline set of capabilities while providing cross-border coordination and cooperation. But this is only a small step towards European cyber resilience. In this landscape, preparedness, shared situational awareness, and coordinated incident response are essential for effective crisis management and cyber-security resilience. This paper presents PHOENI2X which, motivated by the above, aims to design, develop, and deliver a Cyber Resilience Framework (CRF) providing Artificial Intelligence (AI) - assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of OES and of the EU Member State (MS) National Authorities entrusted with cyber-security.

- ***Security shortcomings in healthcare: a preliminary investigation of Data Protection Authorities' decisions***. Nanou, C., Kampyli, M., Crociani, M., & Danilatou, V. (2023). In 19th International Conference on the Design of Reliable Communication Networks (DRCN), DOI: 10.1109/DRCN57075.2023.10108175.

  Abstract: As digital technologies are being more and more deployed to support the healthcare sector, the latter becomes increasingly vulnerable to cybersecurity and privacy risks. The past decades, significant effort has been put into advancing standardization and regulatory frameworks, aiming at protecting healthcare infrastructure and digital applications intended for use in healthcare, along with ongoing research on this field. Motivated by the ongoing research that uses digital applications in the healthcare, which is also conducted in two relevant HORIZON research projects (RETENTION and PHOENI2X), this work aims at providing insights on regulatory compliance challenges faced in this context and exploring respective shortcomings or solutions in practice. To this end, we reviewed decisions of the supervisory authorities within the USA and EU regarding data breaches in the healthcare sector, issued from 1/1/2020 to 31/12/2022, illustrating the most common areas of vulnerabilities and discussing the challenges and the lessons learned.

- ***Identity Management through a global Discovery System based on Decentralized Identities***. Lampropoulos, K., Kyriakoulis, N., & Denazis, S. In CAMAD 2023 - CCI 2023: Cybersecurity of Critical Infrastructures.
  Abstract: Digital identities today continue to be a company resource instead of belonging to the actual person they represent. At the same time, the digitalization of everyday services intensifies the Identity Management problem and leads to a constant increase of users online identities and identity related data. This paper presents DIMANDS2, a framework capable of organizing identity data that allows service providers and identity issuers securely exchange identity related information in a privacy-enabled manner while the user maintains full control over any activity related to his/her identity data. The framework is format-agnostic and can accommodate any type of identifier (existing or new), without requiring from existing services and providers to implement and adopt another new global identifier.
- ***Reviewing BPMN as a Modeling Notation for CACAO Security Playbooks***. M. Zych, V. Mavroeidis, K. Fysarakis and M. Athanatos. (2023) IEEE International Conference on Cyber Security and Resilience (CSR), DOI: 10.1109/CSR57506.2023.10224922.
  Abstract: As cyber systems become increasingly complex and cybersecurity threats become more prominent, defenders must prepare, coordinate, automate, document, and share their response methodologies to the extent possible. The CACAO standard was developed to satisfy the above requirements providing a common machine-readable framework and schema to document cybersecurity operations processes, including defensive tradecraft and tactics, techniques, and procedures. Although this approach is compelling, a remaining limitation is that CACAO provides no native modeling notation for graphically representing playbooks, which is crucial for simplifying their creation, modification, and understanding. In contrast, the industry is familiar with BPMN, a standards-based modeling notation for business processes that has also found its place in representing cybersecurity processes. This research examines BPMN and CACAO and explores the feasibility of using the BPMN modeling notation to graphically represent CACAO security playbooks. The results indicate that mapping CACAO and BPMN is attainable at an abstract level; however, conversion from one encoding to another introduces a degree of complexity due to the multiple ways CACAO constructs can be represented in BPMN and the extensions required in BPMN to fully support CACAO.
- ***The FormAI Dataset: Generative AI in Software Security through the Lens of Formal Verification***. Norbert Tihanyi, Tamas Bisztray, Ridhi Jain, Mohamed Amine Ferrag, Lucas C. Cordeiro, and Vasileios Mavroeidis. (2023). 19th International Conference on Predictive Models and Data Analytics in Software Engineering (PROMISE 2023). Association for Computing Machinery, New York, NY, USA, 33–43. https://doi.org/10.1145/3617555.3617874.
  Abstract: This paper presents the FormAI dataset, a large collection of 112,000 AI-generated compilable and independent C programs with vulnerability classification. We introduce a dynamic zero-shot prompting technique constructed to spawn diverse programs utilizing Large Language Models (LLMs). The dataset is generated by GPT-3.5-turbo and comprises programs with varying levels of complexity. Some programs handle complicated tasks like network management, table games, or encryption, while others deal with simpler tasks like string manipulation. Every program is labeled with the vulnerabilities found within the source code, indicating the type, line number, and vulnerable function name. This is accomplished by employing a formal verification method using the Efficient SMT-based Bounded Model Checker (ESBMC), which uses model checking, abstract interpretation, constraint programming, and satisfiability modulo theories to reason over safety/security properties in programs. This approach definitively detects vulnerabilities and offers a formal model known as a counterexample, thus eliminating the possibility of generating false positive reports. We have associated the identified vulnerabilities with Common Weakness Enumeration (CWE) numbers. We make the source code available for the 112,000 programs, accompanied by a separate file

containing the vulnerabilities detected in each program, making the dataset ideal for training LLMs and machine learning algorithms. Our study unveiled that according to ESBMC, 51.24% of the programs generated by GPT-3.5 contained vulnerabilities, thereby presenting considerable risks to software safety and security.

2.4.4 Visual and identity branding (PHOENI2X brand book)

A complete graphic identity to communicate the main concepts of the PHOENI2X project has been designed. This simple, useful and consistent graphic identity helps the consortium to communicate the project messages more effectively and is the base for communicating towards the outside world. Graphic identity involves the use of logos, type fonts and colours to create an image easy to recognize by the audience. All material that will be developed will follow this graphical identify. Consistent graphic identities allow the target audience to easily identify and recognize the PHOENI2X project. For this reason, it is essential that all material distributed by the project partners maintain the project's identity.

2.4.4.1 Logo

The PHOENI2X project logo was designed to be used in all project documents, publications, and presentations, as well as in all digital presence of the project (project portal, social media channels, etc.). The logo is the main graphic identity element and the key to build a successful graphic identity, as well as an effective communication. The logo is available in multiple resolutions, appropriate for different purposes. The purpose of the PHOENI2X logo is to draw attention and represent the project context in an easy to remember image. Screen shots of the PHOENI2X logo are illustrated in Figure 11: PHOENI2X logo below:

Figure 11: PHOENI2X logo

2.4.4.2 Templates

All reports, deliverables, presentations, newsletters, press releases and PHOENI2X material will use the PHOENI2X templates to obtain the corporate identity of the project. The templates are available from the internal project portal, these include:

1. Presentation template (.pptx)
2. Deliverable template (.docx)

2.4.5 Website

The PHOENI2X website is one of the main dissemination tools of the project. The current version of the website follows the project´s graphic identity and presents the project's overview, including objectives, pilots and project partners. Developed using WordPress[25], the website has been designed and implemented by UPC. The final version was released in September 2022. The sections of the PHOENI2X website are: Project, Pilots, Blog, News & Events, Results and Contact.

[25] https://wordpress.com/

The website follows the EU recommendation regarding usability and accessibility[26], and it includes the logo of the European Commission. Figure 12 shows the PHOENI2X Home page.

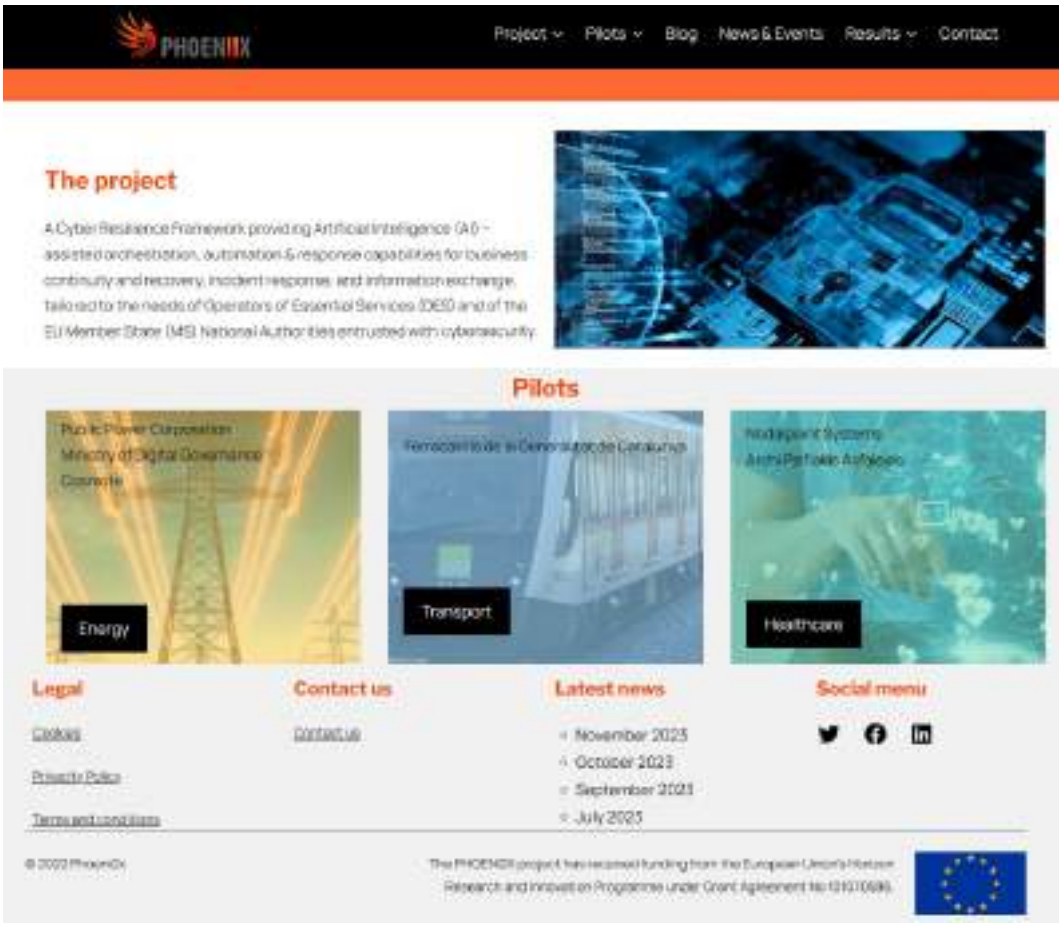


Figure 12: PHOENI2X website

Figure 13 to Figure 19 shows the main statistics regarding the PHOENI2X website, from its creation in October 2022, to November 30, 2023. In Figure 14, an interesting finding is the impact that has the publication of the PHOENI2X Press Release in all Greek mass media leaded by PPC. Figure 18 shows the top downloads, headed by the PHOENI2X Brochure, 1st Newsletter, and 1st Press Release. Figure 19 shows the most visited pages of the PHOENI2X website, the top four are the main page, Promotional Material, Blog and News and Events.

Figure 13: Visits statistics - first year of the project

Figure 14: Visits statistics – M12-M17

[26] Web Accessibility | Shaping Europe's digital future (europa.eu)

Figure 15: Number of visits of the last year (November 30, 2023) *Figure 16: Top Referring (November 30, 2023)*

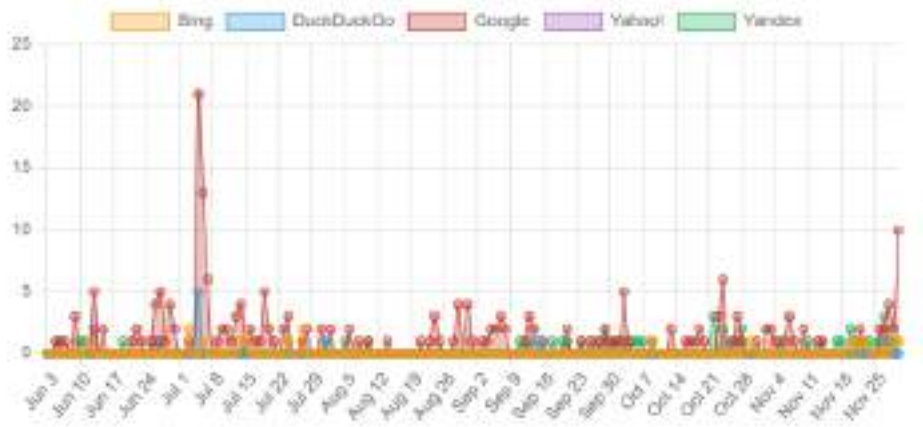


Figure 17: Search engines referrals (November 30, 2023)

Figure 18: Top downloads (November 30, 2023) *Figure 19: Most visited pages (November 30, 2023)*

2.4.6 Social Networks

One important channel for disseminating and communicating PHOENI2X results and news are the social media. In the PHOENI2X project a Twitter account, LinkedIn page, and Facebook page were created, see Figure 20.

Figure 20: PHOENI2X Twitter account (left), LinkedIn page (center), Facebook page (right)

Initially, a ResearchGate project page for PHOENI2X has been created, however by the end of March 2023 all project pages in ResearchGate were removed by the same social network.

The three PHOENI2X accounts are used to disseminate PHOENI2X work, publishing news related to PHOENI2X such as meetings, scientific publications, workshops, etc. On LinkedIn the target audience is slightly different from the Twitter and Facebook audience. LinkedIn is focused on a more scientific and companies' audience, while Twitter is addressed to a more general audience, but not limited to it.

Currently the data for the three accounts is:

- LinkedIn:
  - Link: https://www.linkedin.com/company/PHOENi²X/
  - Number of posts: 80
  - Number of followers: 184
- Twitter:
  - Link: https://twitter.com/PHOENi²XProject
  - Number of posts: 126
  - Followers: 90
- Facebook:

- Link: https://www.facebook.com/PHOENi²X/
- Number of posts: 82
- Followers: 50

Figure 21 shows the most appreciated LinkedIn posts during the first 18 months of the project, being the posts with more impressions the related with the plenary meetings of the project and followed by the newsletters and paper presentations in conferences.

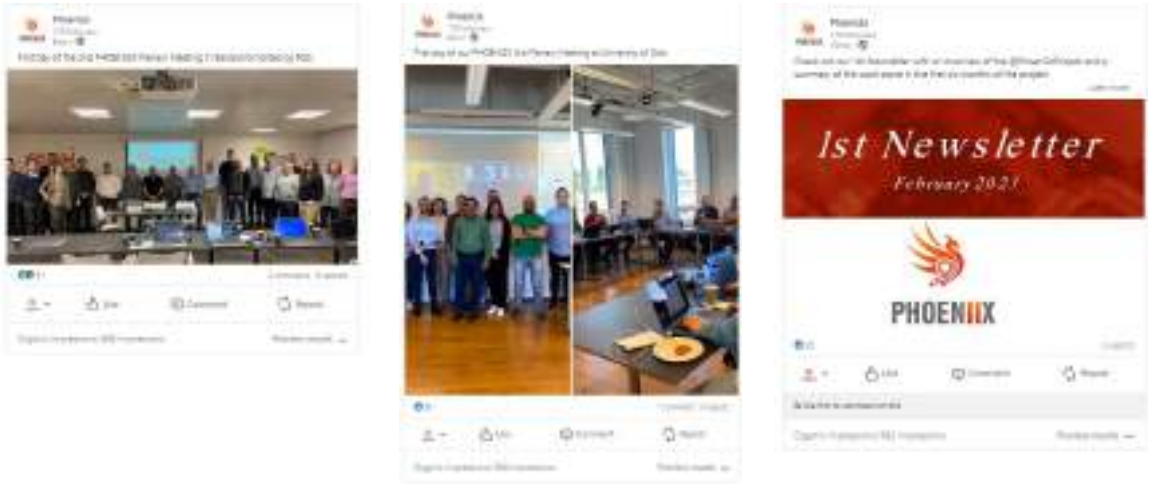


Figure 21: Most appreciated LinkedIn posts (November 30, 2023)

2.4.7 Blog

PHOENI2X consortium agreed on publishing a blog to spread PHOENI2X to a more general audience. The blog posts are shared through the project website (see Figure 22), and are promoted in the social networks (LinkedIn, Twitter and Facebook). Blog posts in PHOENI2X are published monthly and are produced by all the partners with the objective of promoting project results and ignite interesting conversations.

Figure 22: Blog in PHOENI2X website

The first blog entry has been generated by the technical coordinator and provide an overview of the PHOENI2X framework. Following blogs cover a variety of topics related with PHOENI2X research topics. Table 7 below summarizes the blog entries produce during the first period of the project.

Table 7 PHOENI2X Blog entries

Partner	Date	Title
SANL	October 2022	Towards Cyber Resilience of European Operators of Essential Services – The PHOENI 2 X project
UPAT	November 2022	PHOENI2X at CyberHOT Summer School 2022
ATOS	December 2022	Cyber Threat Intelligence, the way to prevent and combat cyber threats
AEGIS	January 2023	How can AI be used to enhance Cyber Security of Essential Services?
WS	February 2023	Reducing the risk of cyber-attacks by incorporating cyber security features in IoT solutions
SEA	March 2023	The Influence of Artificial Intelligence on Social Engineering Attacks – The Attackers' Perspective
NCSA	May 2023	Regulatory compliance supported by PHOENI2X
UPC	June 2023	Use of Transfer-Learning to improve the detection of zero-day attacks
NPS	July 2023	The Rise of Supply Chain Attacks
DSA	August 2023	Safeguarding the Critical Information Infrastructures though PHOENI2X framework
SANL	September 2023	Increased OES preparedness, through PHOENI2X Cyber Range - enabled realistic scenario assessment & training
EUNL	October 2023	EU's proposal for an AI Act – the world's first initiative on regulating Artificial Intelligence
AEGIS	November 2023	Designing Intuitive and Secure User Interfaces in Cyber Resilience Frameworks
UiO	December 2023	Code Red: A large scale study on ChatGPT generated code vulnerabilities

2.4.8 Newsletters

The PHOENI2X Newsletter is used to carry out direct proactive communications to the targeted stakeholders, the European Commission, researchers and potential interested investors. At this stage of the project three Newsletters have been produced with the following objectives:

- 1st Newsletter:
  - Present the project objectives
  - Involve stakeholders in the project activities and workshops
  - Date: February 2023
- 2nd Newsletter
  - Present the PHOENI2X framework
  - Present the main achievements of the first year of the project
  - Date: July 2023
- 3rd Newsletter
  - Present the PHOENI2X use cases

- Present the main achievements of the last five months of the project
- Date: November 2023

2.4.9 Press releases

PHOENI2X press releases are used to disseminate the project by informing about the real benefits that PHOENI2X can offer to the stakeholders (general public and civil society organisations, scientific community, industry and government). Three of the eight Press Releases of the project will be published by the Use Case owners in national magazines and/or newspapers of the partner country. During the first period of the project PCC published a Press Release in all Greek mass media presented the PHOENI2X project and this action has a great impact in our social networks and also in the visits to our website (as we have presented in section 2.4.5).

During this first period of the project two press releases have been published.
1st Press Release:

- Present the PHOENI2X project.
- Date: November 2023

2nd Press Release

- Present the PHOENI2X to broad audience in Greece.
- Date: July 2023

2.4.10 Dissemination & communication toolkit

This section presents the printed/published online dissemination material for the PHOENI2X project. This material is used as brochure, posters and infographics in face-to-face meetings. It is available in the PHOENI2X website and repository to be freely used by the partners.

2.4.10.1 Brochure

The main objective of the brochure is to provide our audiences with an attractive and written project overview and a summary of the main project objectives and characteristics.

Figure 23: PHOENI2X brochure

Two brochures for the PHOENI2X project have been produced in form of a two-pages document. The first, see Figure 23 (left side), briefly describes what is PHOENI2X and the objectives. While the second, see Figure 23 (right side), briefly describes the use cases of the project. Both brochures are available in the repository and published in the PHOENI2X website.

2.4.10.2 Poster

The main purpose of the poster is to catch the audience attention. The PHOENI2X poster, see Figure 24, is designed to give a clear and concise description of the project to interested parties.

Figure 24: PHOENI2X poster

2.4.10.3 Infographics

The PHOENI2X infographic follows the definition: "*Infographic is a collection of imagery, charts, and minimal text that gives an easy-to-understand overview of a topic*."

Figure 25: PHOENI2X roll-up banner

Considering this definition during the first period of the project the consortium has produced three infographics. Figure 25 shows one of them, which present the project as a whole. This infographic media aims to facilitate the understanding of the PHOENI2X features and benefits and was printed is a roll-up banner.

2.5 Monitoring and Evaluation of Dissemination and Communication activities

The success of the dissemination and communication activities of the PHOENI2X is assessed through several key performance indicators (KPIs). These KPIs were defined in the grant agreement (see Table 4) for the whole duration of the project, and a plan for their achievement is proposed in Table 5 and Table 6. In this section, Table 8 and Table 9 monitors the evolution of the dissemination and communication activities in the project showing the activities done during the first year of the project and the six first months of the second year, while in parenthesis are detailed the KPIs for the first and second year of the project.

Regarding the KPIs in Table 8, the number of current published journals with ACK to the project is 2; and the impact factor of these journals is:

- Sensors, 23(3), 1252. (JCR 3.9 Q2)
- Journal of Network and Systems Management (JCR 3.6 Q3)

During the second period the project the consortium plans to publish in 6 or more journals, due to the maturity of the research developed in the project, fulfilling this KPI.

Regarding the papers in conferences or workshops the number of published papers is 8, being some of them of ranks[27][28]:

- ARES'22 (rank B)
- Big Data 2022 (rank B)
- CAMAD 2023(rank B)
- DRCN 2023(rank B).
- PROMISE 2023 (rank C).

During the second period of the project the consortium plans to publish in 7 more, fulfilling this KPI.

Finally, in terms of organized workshops the consortium has already accomplished the proposed KPI with already 2 co-organized workshops, and 2 summer schools co-sponsored.

Table 8 Dissemination KPIs M18

Activity/Measures	**Targets**		**Expected Impact**
	Y1	**M18 (Y2)**	
Journal publications	2(2)	0(2)	Validation of the project findings and results. Promotion of the results to scientific communities. Exchange of knowledge with relevant communities and initiatives.
International conferences	2(2)	6(6)	
Special issues/ Book chapters	0(0)	0(2)	

[27] https://scie.lcc.uma.es/ratingSearch.jsf
[28] https://www.resurchify.com/

Workshops/Special sessions	2(1)	1(1)	Increased collaboration with other initiatives and projects for joint research, information exchange and dissemination. Liaisons. Validation of project's concept, findings and progress
EU-focused event	0(0)	0 (0)	
Technical, Academic, Industrial events	1(1)	2(1)	Knowledge exchange with relevant communities and initiatives. Promotion of results to relevant communities and initiatives.
Interactive face-to-face networking	0(0)	1(1)	
Collaboration with other projects	2(1)	2(1)	Contact to external stakeholders to promote PHOENI2X solutions. Increased awareness.
Collaboration OES stakeholders	0(0)	0(0)	
Collaboration with cybersecurity policy	0(0)	1(1)	

Table 9 Communication KPIs M18

Activity/Measures	**Activity/Measures**		**Measurable indicators and target value**
	Y1	**M18 (Y2)**	
Project website Deployed in M2 Accesses	3228 (1000)	4125(1000)	Main online information channel. Communication of project news, events and results. Increased awareness.
Downloads	164 (100)	556(100)	
Video clips	0(0)	0(1)	Attainment of interest of general public active in social media. Drive engagement with the project.
Social media Facebook Followers	35(35)	50(50)	
Posts	50(30)	32(30)	
Twitter Followers	66(50)	90(75)	Attainment of interest of stakeholders active in social media. Sharing knowledge with other projects and initiatives. Drive engagement with the project.
Posts	52(30)	74(30)	
LinkedIn Connections	131(100)	184(150)	
Posts	46(30)	34(30)	
Press releases	2(2)	1(3)	Promotion of results to relevant communities and initiatives. Proactive communications to the targeted stakeholders, the European Commission, researchers.
Newsletters	2(2)	1(3)	
Flyers/ Brochures	1(2)	1(3)	Promotion of the project to stakeholders and scientific community. Attainment of interest. Drive engagement with the project.
Posters	1(2)	1(3)	
General Public	0(0)	0(1)	Attainment of interest of general public. Drive engagement with the project.

2.6 Dissemination and communication plan for next period

During the second year of the project the consortium will plan at least the following dissemination and communication activities:

- Publications: 6 journal papers, 7 international conferences, 5 special issues or book chapters
- 1 demonstration in an EU focused event
- 3 interactive face-to-face networking EU event
- 1 meeting with OES stakeholders per UC country
- 1 meeting with cybersecurity policy makers at national and EU level
- 2 videos
- 18 blog entries
- 5 Newsletters and 5 Press Releases
- 6 brochures and 6 posters
- 2 articles/interviews to national magazines in Greece, Cyprus and Spain

Apart of these planned activities, the website and social networks will PHOENI2X will be continuously updated. On the other hand, after 18 months of work, the maturity of the project will be enough to get benefits in terms of scientific publications, conference and journals, both individually and jointly between several partners.

Finally, the individual plans for dissemination and communication of the PHOENI2X partners are detailed below.

UPAT

UPAT will work towards the dissemination and transfer of results through a series of activities and actions. Continuing the work that has already been done, its main focus will be to publish more research papers and scientific results in relevant conferences, workshops, scientific journals etc. Furthermore, UPAT has already contributed to the organization of the project's first workshop (IOSEC 2023) and plans to be involved in the organization of at least two more. It has disseminated the project in various information days (Infocom world 2023), expositions (TIF - HELEXPO), summer schools (CYBERHOT), scientific workshops (CyberHunt) and will continue these activities until the end of the project. It will further promote PHOENI2X through its communication channels, and will create content to support project's website, blog and social media. Finally, since the UPAT group is leading one of ETSI's Software Development Group (Openslice), it will engage with the Standardization Community to investigate potential contributions.

SANL

SANL disseminates the PHOENI2X project, its results and their impact on the company's product & service portfolio via the project's relevant channels, but also through the companies' own communication channels (e.g., own website, professional social media). SANL's employees also have a strong academic background and, therefore, participation in academic venues to promote the project's results are already being carried out (e.g., through publications, workshops) and are expected to intensify as the project's outputs mature.

UPC

UPC as the task leader of dissemination and communication, will continue coordinating the overall set of activities and actions related to communication and dissemination. In this leadership role, UPC will gather all the information about dissemination actions from all partners, such as scientific publications, blog entries, attendance of events and others. Fruit of this activity, UPC will continue updating news and events on PHOENI2X website, as well as posting on LinkedIn, Twitter and Facebook. UPC is also in charge of the production of the Newsletters of the project. From the research point of view, UPC plans to write 2 papers in journals and 2 more submitted to conferences.

COSM

For the forthcoming period until the end of the PHOENI2X project, COSMOTE plans to create opportunities (via face to face meetings, e-mails, presentations) to disseminate the goals, objectives and innovations of the project internally to the company Departments entrusted with security and business continuity as well as those responsible for the security solution for enterprises provided as a service by COSMOTE. It also plans to utilize the company dissemination channels to reach hundreds of employees to raise awareness on the state-of-the-art technology areas handled by the PHOENI2X project (AI, tools for cybersecurity, etc.); thus, contributing to the technology superiority that is one of the company strategic pillars. The project will be also included in the annual sustainability reports of COSMOTE and the DT Group which will give it a lot of recognition in Greece and abroad. In addition, COSMOTE will maintain the project dedicated webpage in the official company portal during the entire project duration and after the project end. Last but not least, COSMOTE will participate in all the dissemination and communication activities organized by the consortium, incl. conferences/workshops, posts in the social media, videos, publications, etc.

FGC

During the following project period until its completion, FGC will support the project's communication & dissemination activities, as has already been done, by participating in events, workshops and meetings presenting the results and opportunities of Phoeni2x, communicating the projects' results though FGC social media accounts, mainly LinkedIn, and disseminating the possibilities, achievements, and challenges of cybersecurity in the railway sector. Phoeni2x project will be included also in the internal annual reports of FGC, and internal newsletters, documents received by more than 2.000 employees.

PPC

PPC will support the project's communication & dissemination activities by a) participating in industrial events and expositions, particularly at Enlit Europe, b) disseminating/communicating the project results through PPC's social media channels, c) collaborating with technology providers of the project for scientific publications in the context of the UC1 results, d) promoting the results of PHOENI2X internally in PPC group and relevant stakeholders, including the Hellenic Distribution Network Operator (HEDNO) - the Greek DSO, e) contributing to potential white papers describing the results and impact of PHOENI2X, especially for the energy sector and the advanced metering infrastructure, f) publishing blog posts to the PHOENI2X website, according to the blog post schedule.

WSE

WSE has already and will continue supporting the project's communication and dissemination activities by a) participating in events and presenting the project's outcomes, b)

disseminating/communicating the projects' results though WSE's social media accounts and its corporate website, c) contributing to white papers, blog posts and articles describing the results and the impact of them especially at the railway sector and beyond.

AEGIS

AEGIS will support the project's communication & dissemination activities by i) participating in events and presenting the main outcomes of PHOENI2X at appropriate international venues, ii) helping organize events hosted by the project in order to promote the discussion on the topics covered within it, iii) publishing research papers and scientific work in conferences/workshops/journals in cooperation with the other partners when possible, iv) contributing to the project website and social media channels, v) promoting PHOENI2X via the company's website and social media accounts and vi) participating in industrial workshops/expositions/fora (e.g. FIC forum) to promote PHOENI2X's accomplishments in various ICT communities.

SEA

SEA is committed to enhancing cybersecurity training for PHOENI2X through a blend of innovative methods and measurable outcomes. Central to our strategy is the provision of both physical and digital serious games, designed to offer immersive and interactive training experiences. These games are tailored to meet specific learning scenarios, ensuring that content is highly relevant to the trainees' needs.

EUNL

The project's communication and dissemination activities will be supported through EUNL's and the project's communication channels as well as activities, including participation in scientific conferences/workshops and journal publications, with the aim of raising the awareness of the scientific community, industry, policymakers, and the general public regarding the PHOENI2X project and its significance. Moreover, please note that, in the context of PHOENI2X dissemination, we have a poster entitled "Standardization: AI Act's Cornerstone" to be presented at the ETSI AI conference in February. Even though it is only indirectly relevant to the particular project, the latter will be explicitly mentioned and acknowledged as the sponsor on the poster.

ATOS

ATOS will actively contribute to the project's online presence and social media platforms, and advocate for PHOENI2X through ATOS's website and social media channels to enhance the project's visibility. ATOS will be involved in the creation of scientific articles that allow the purpose of the project to be made known. Furthermore, posts regarding topics related to the project will be written for its website, as they will provide visibility to the industry the project is focused on.

APS

APS will work towards the dissemination and transfer of results through a series of activities and actions. Continuing the work that has already been done, its main focus will be transfer the knowledge gained through the project to various Standards Developing Organizations and related standardization efforts. APS will further promote the project through the participation in project dissemination activities, the propagation of the project results through the social media of the organization and contribute in the implementation of blogs.

NPS

NPS will participate in the PHOENI2X communication & dissemination activities through (i) contribution to informative material (including posters, flyers, videos), (ii) preparation of newsletters

and press releases, (iii) promotion of the project activities in social media (e.g., LinkedIn, facebook, Twitter), (iv) engagement in events (conferences, workshops, industrial events, expeditions) and preparation of relevant material (e.g., papers), (v) participation in and publishing of research papers for international journals.

UiO

UiO will work towards disseminating and transferring results through a series of activities and actions. Being an academic partner, UiO will focus on publishing further PHOENI2X research in top academic and industry venues. Shortly, on Dec. 17 2023, the annual Workshop on Cyber Threat Intelligence and Hunting (CyberHunt 2023) under the IEEE Big Data Conference will be held in Sorrento, Italy, with the consortium present to communicate PHOENI2X results. Our plan is also to co-organize and contribute research findings in CyberHunt 2024.

UiO will continue contributing while also promoting and demonstrating the added value proposition of PHOENI2X in standardization bodies (see section 4) and conferences. For 2024, we already have one participation confirmed in the highly recognized EU conference "EU Cyber Acts", where we will discuss our contribution to the OASIS CACAO Security Playbooks standard and its position in the European regulatory dimension[29]. UiO is also very active on social media, with a strong following on Linkedin that is used to promote PHOENI2X dissemination and communication material.

NCSA

NCSA will support the project Communication & Dissemination activities in the following ways: i) Contributing in the development of dissemination material. ii) Supporting and attending events organized by the project, that promote the covered concepts. iii) Helping increase the project impact on social media. iv) Promoting the project and its outcomes to the national ecosystem.

DSA

DSA will support the project's communication & dissemination activities by: i) presenting the main outcomes of PHOENI2X at cybersecurity related events, ii) promoting PHOENI2X via the organization's website and social media accounts, iii) informing the critical infrastructure organizations for the PHOENIX2 via email and presentations.

[29] https://eucyberact.org/session/european-cross-border-cybersecurity-operations-collaboration-through-the-lens-of-the-cacao-standard-b22d/

3 EXPLOITATION

3.1 Objectives of Task 6.2. on exploitation

This task aims to facilitate the sustainability and impact of PHOENI2X. To achieve this the following steps have been mapped out.

- Start as a baseline from the exploitation plan drafted during the proposal submission period.
- Design a method to collect updated information on the exploitation potential of the PHOENI2X outcomes. This method will allow us to gain an overview of the exploitable and key exploitable results (ERs and KERs) of the project.
- Based on the information collected on ERs and KERs, identify their market prospects in the short and long term, develop a business plan and a market strategy.

The activities described above have started in month 9 of the project and will be completed by the end of the project.

The plans included in this version of the document will be updated as needed and their final version will be presented within D6.2 – Final report on Dissemination, Exploitation, Standardization & Sustainability, to be released on M36 of the project.

3.2 Initial Exploitation Plan

The project proposal included an initial exploitation plan for the PHOENI2X results. To present this plan, an initial business model canvas was created for PHOENI2X. This initial version of the canvas is presented in Figure 26:

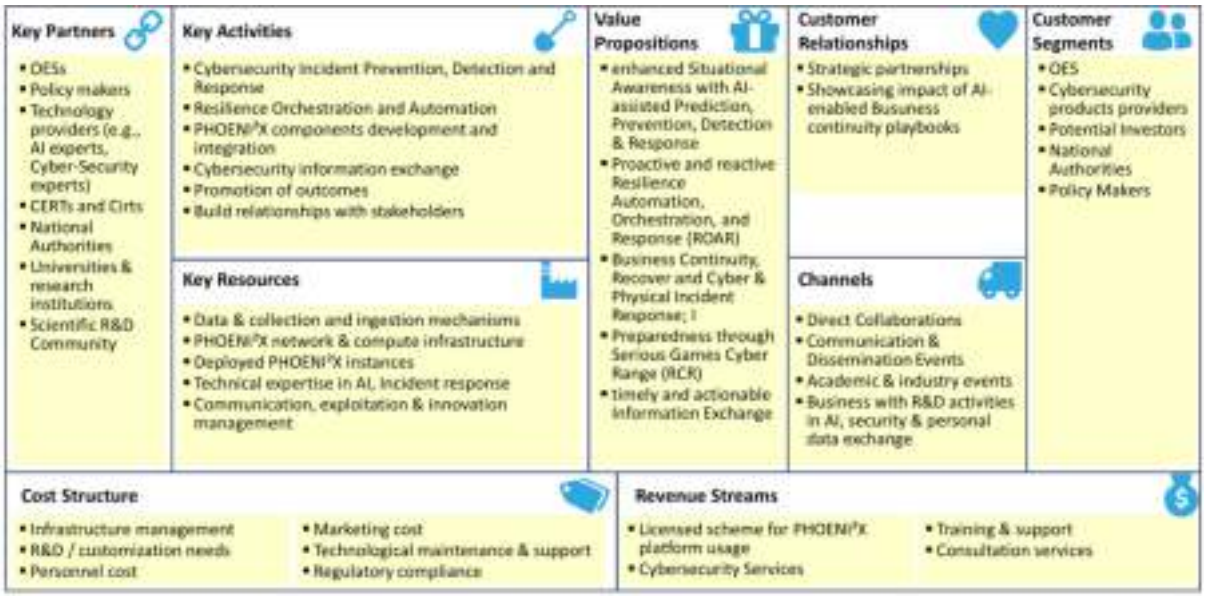


Figure 26: The initial business model canvas for PHOENI2X as presented within the proposal documents.

Two sets of plans have been set out within the project proposal.

Project exploitation plan. Specifically, PHOENI2X's exploitation plan incorporates a three-layer architecture, defining distinct exploitation domains for each partner to engage with, based on expertise and role in the project. At a research layer, results and innovative AI tools will be applied in the general AI research area, currently more active than ever in targeting for explainable AI along with black-box AI exploration. The second layer is related to technological exploitation, including tools and services implementation, translating innovative research

outcomes into exploitable end-products. The final layer includes the sustainable development and commercial exploitation of end-products within technical and OES areas to which PHOENI2X end-users are active.

Individual exploitation plans. Each partner has provided a draft exploitation plan for their involvement within the PHOENI2X project. These plans are depicted below in Figure 27

Partners		Exploitation Strategy
ACADEMIC INSTITUTIONS	UPAT, UPC, UiO	Academic partners will exploit the outcomes if PHOENi²X for the re-utilization of the research and technological know-how acquired for the future research activities and services. They will also seek to create additional teaching material for both graduate and post-graduate courses. Finally, they will explore exploitation opportunities including: - Transferring results and know-how into further EU projects. - Transferring results and know-how into national or industrial research projects. - Developing new services based on the prototypes, methods, and tools
BUSINESS SECTOR	SANL, WS, AEGIS, SEA, EUNL, ATOS, APS	Business partners will use the outcomes of PHOENi²X for strengthening their services and product portfolio. This will be possible by enhancing current products or by creating new services to support their client base. Using the knowledge gained in the project, business partners will have the opportunity to create synergies, demonstrate their technological offerings and increase their business capacity.
OES INSTITUTIONS, OPERATORS & AUTHORITIES	PPC, COSM, NCSA, FGC, NPS, DSA	These organizations will participate to the project by executing the use cases and relevant validation and cross-validation activities. Through the adoption of the PHOENi²X results, these institutions will enhance services they provide to their clients, gain benefits in carrying out their mission, while gaining hands-on experience with state-of-the-art technologies for their technical experts and professionals.

Figure 27: The initial Partner's exploitation plans as presented within the proposal documents.

3.3 Exploitation design methodology

To effectively design the exploitation plans (project and individual), it is necessary to design a methodology to support and manage the relevant process.

This methodology should cover the following steps:

1. Data collection. The collection of information regarding the exploitable results and information on the market.
2. Input ranking. The definition of criteria for the ranking of the identified exploitable results with the aim of identifying the Key exploitable results.
3. Market analysis. An analysis of the desired characteristics of the solutions, as described by the market.
4. Definition of strategies. Definition of strategies that will allow the exploitation of the Key Exploitable results of the project and the fulfillment of the exploitation goals of the project partners.

The actions defined as part of the strategies and plans shall be implemented in the timeline prescribed. The actions will also involve planning and initial activities regarding intellectual property rights, privacy protection and others as needed. The plans and strategies should be reviewed and updated as needed

based on the results of these actions, the feedback of interested parties and the changes during the project's lifetime.

3.3.1 Data Collection

Exploitation means the use of results in further research and innovation activities other than those covered by the action concerned, including inter alia, commercial exploitation such as developing, creating, manufacturing, and marketing a product or process, creating and providing a service, or in standardization activities.[30]

Exploitation focuses on the actual use of the results, translating research concepts into concrete solutions that have a positive impact on the public's quality of life.

According to the Horizon 2020 guide text[31], a result is defined as:

"Any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights".

Exploitable Result (ER) is considered any form of intangible project result (technical consulting, business consulting, system integration capacity), or tangible result (software component, library, tool, prototype, service suite, etc.).

A Key Exploitable Result (KER) is an identified main interesting result (as defined above) which has been selected and prioritized due to its high potential to be "exploited" – meaning to make use and derive benefits- downstream the value chain of a product, process or solution, or act as an important input to policy, further research, or education.

The first step of the process is to provide a structured way for the partners to identify exploitable results.

A document was created (Document: ERs Identification), in which each partner was requested to provide the relevant exploitable results information.

The document consists of the following sections:

1. Basic Information. Requesting information on the partner, the name of the Exploitable result, the type of the result, its main functionalities, the expected project month of completion and the possible exploitation path.
2. Assistance information. Requesting information on the type of assistance needed by the partner to achieve the effective exploitation of the result.
3. Technical maturity. Requesting information on the technical maturity of the result based on the TRL scale.
4. Market demand. Requesting information on the market demand and readiness level of the market.
5. Value proposition canvas. Requesting information on the fit of the result for the market following the Value Proposition Canvas initially developed by Dr Alexander Osterwalder.

[30] Online manual, European Commission, Dissemination and exploitation of project results (https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=1867974)
[31] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results_en.htm

The template document used is presented in Annex A of this document.

Results of the data collection:

Table 10 depicts the Exploitable Results identified by the project partners during the first iteration of the exploitation results data collection process (June-August 2023). A total of 21 Exploitable Results were identified during this first iteration of exploitable results data collection.

Table 10 Exploitable Results identified by the project partners (first iteration)

Partner Name	Exploitable Result (ER)	Type of ER
ALL	The PHOENI2X Solution	Service / Solution
AEGIS	Forensics Vizualisation Toolkit (FTV)	Software
ATOS	SMIR exploitable results. Integration with other tools in the project and improvement of SMIR capabilities.	Software
ATOS	TINTED exploitable results. Integration with other tools in the project and improvement of TINTED capabilities.	Software
ATOS	CERCA exploitable results. Integration with other tools in the project and improvement of CERCA capabilities.	Software
COSMOTE	Obtain knowledge about the PHOENI2X security solution that could be potentially partly utilized to enhance/expand the Managed Security Services solution that is currently being offered by COSMOTE (Solution-as-a-Service) to its business customers.	Knowledge
DSA	Attack Prediction and Response for Critical Information Infrastructures (OES)	Software
FGC	Cyber protection of the data generated by the sensors to control the railway infrastructure.	Service
NCSA	Raise entities awareness and compliance level, regarding NIS2 requirements on Incident alerting and reporting.	Compliance process
NODALPOINT	Security Provider Control Plane (SPCP)	Software
SANL	The SPHYNX Cyber Range tool offers cyber security training that covers a comprehensive spectrum of known and emerging security and privacy threats and is tailored to the particular security and privacy risks of different organizations.	Deployment of a novel product and service
SANL	ROAR, which builds upon the SPHYNX Incident Response tool offers a security orchestration, automation, and response (SOAR) solution supporting the prevention, detection, investigation, and response to cyber security attacks. To do so, the tool uses executable playbooks specified according to the OASIS CACAO standard	Deployment of a novel product and service
SANL	The SPHYNX Security and Privacy Assurance Suite (SPHYNX SPA Suite) is an integrated suite of tools that provides comprehensive cyber security risk detection and management for enterprise systems.	Deployment of a novel product and service

SANL	The UEBA component of PHOENI2X, built upon the SPHYNX Security Analytics Tool, that supports model-driven data analytics for security.	Deployment of a novel product and service
UPAT	Deception Tools (Honeypot) A deception tool, such as a honeypot, is a cybersecurity mechanism designed to lure attackers into a controlled environment. By imitating vulnerable systems, honeypots enable the collection of valuable insights into attack techniques, enhancing threat intelligence and improving security defenses.	Software
UPAT	Academic and Research Advancements through Project Outcomes UPAT will focus on utilizing the project outcomes to enhance its academic and research activities. This includes a) developing new or improving existing courses, labs, and seminars on security that incorporate cutting-edge research, innovative tools and platforms etc. b) cybersecurity awareness training activities c) fostering collaborations and creating funding opportunities to strengthen academic excellence etc.	Knowledge
APS	Knowledge from the implemented software and project outcomes.	Knowledge
APS	Standards development related to the outcomes of the project and in particular the Emergency management - Incident situational reporting for critical infrastructures (CWA 18024) and Semantic layer definition and suitability of OASIS EDXLCAP and OASIS EDXL-SitRep standards for crisis management in critical infrastructures (CWA 18028)	Contribution to standards
SEA	Addition of relevant scenario within the service of the organization "INTERACTIVE SOCIAL ENGINEERING TRAININGS"	Addition to service
EUNOMIA	Knowledge on legal and regulatory requirements of the OES in different counties	Knowledge
UiO	Standards development and in particular the OASIS Threat Actor Context (TAC) ontology.	Standards

The information contained within table 10 was processed and statistical information regarding the type, the exploitation path, timeline, and the maturity of the exploitable results were extracted.

Figure 28 depicts the statistical information per exploitable result type.

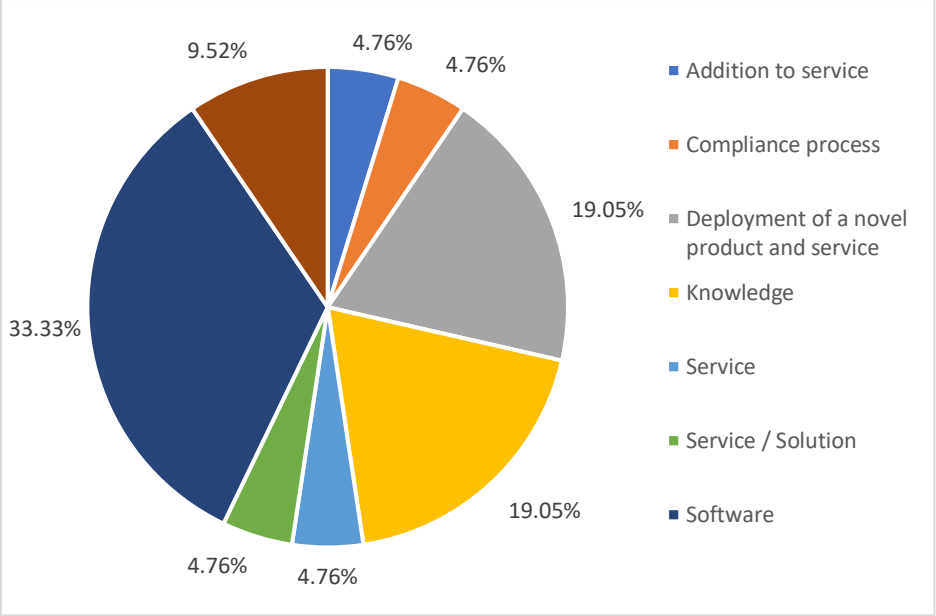


Figure 28: Types of Exploitable Results identified by the project partners (first iteration)

As seen in Figure 28, most of the exploitable results identified by the project partners are software (8 instances ≈33% of all identified exploitable results during this first iteration). The rest of the types, in a descending sorting order are: Knowledge (19%), Deployment of a novel product or service (19%), Contribution to standards (9,5%), and addition to service, compliance process, service and service / solution are all equally at 4,8%. Figure 29 depicts the statistical information on categories of exploitation paths. The main categories identified[32] are:

Utilization. This term incorporates activities related to the usage of exploitable results. Within the project context, the PHOENI2X solution may be used by the entities participating in the project pilots (OES) or may be used by the national authorities to provide related services to the critical or important infrastructures they supervise.

Future Research. This term is used to indicate that part, or all of the exploitable result will be used by the partner as ground for future research.

Commercial Use. This term incorporates activities related to the commercialization of the exploitable results. It should be noted that this is different from utilization in the respect that in this case, a commercial license will be used to provide the solution to the end user entities (which shall not be entities already involved in the project).

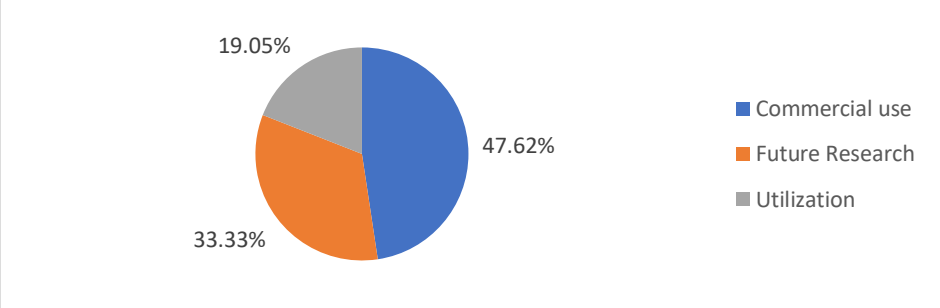


Figure 29: Exploitation paths of Exploitable Results identified by the project partners (first iteration)

[32] These categories have been defined by the project team as appropriate based on the scope and context of the PHOENi²X project.

As seen from Figure 29, most of the exploitation results are planned to be utilized (47,6%). The other two categories of exploitation paths follow with "Future Research" identified in 33,3% of the cases and "Utilization" in the 19% of the cases. It should be noted that a partner may exploit through different parts the exploitable result. This combination of paths, although recorded within the relevant files, is not depicted within the above figures and statistical information.

Figure 30 depicts the statistical information on the expected delivery months of the exploitable results.

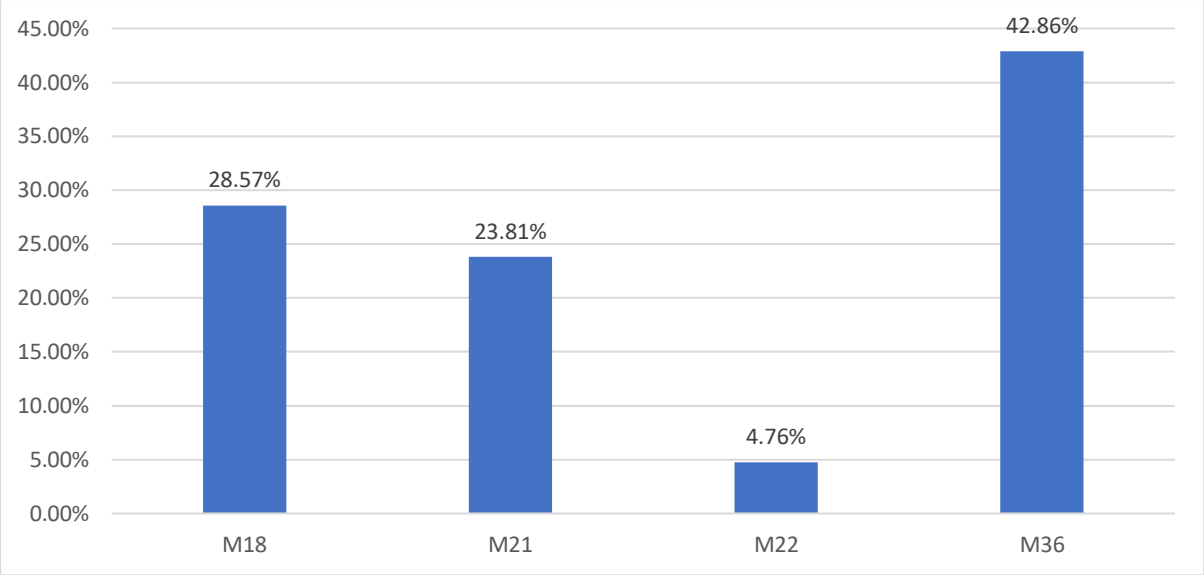


Figure 30: Expected delivery months of Exploitable Results identified by the project partners (first iteration)

As seen from Figure 30, the exploitable results of the project start from month 18. The majority of the exploitable results shall be extracted at the end of the project (M36). Almost 29% of the exploitable results are extracted in M18 and the rest are split between months M21 and M22.

Table 11 depicts the identified exploitable results identified within the first iteration of the data collection process. This list includes only exploitable results of the types: Software, Service, Service/Solution, Compliance process and Deployment of a novel product and service. This means that the types "Knowledge" and "Standards" are not included. This decision was made by the project team since these results cannot easily be depicted based on the standard TRL level definition. (International Organization for Standardization (ISO), 2013) [33].

Table 11 Exploitable Results identified by the project partners (first iteration)- types Software, Deployment of a service and product, Compliance process and Service – with their technical maturity levels

Name and description of the Exploitable Result	Type of result	Technical maturity of the ER at the start of the project	Current technical maturity of the ER	Envisioned technical maturity of the ER at the end of the project

[33] International Organization for Standardization (ISO). (2013). ISO 16290:2013(en) - Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment. Geneva: International Organization for Standardization (ISO).

The PHOENI2X Solution	Service / Solution		2	4
Forensics Vizualisation Toolkit (FTV)	Software	5	5	7
Enhanced CERCA	Software	4	4	5
Integration and improvement of SMIR	Software	4	4	5
Integration and improvement of TINTED	Software	3	3	4
Attack Prediction and Response for Critical Information Infrastructures (OES)	Software	1	3	9
Cyber protection of the data generated by the sensors to control the railway infrastructure.	Service	4	5	7
Raise entities awareness and compliance level, regarding NIS2 requirements on Incident alerting and reporting.	Compliance process	1	2	6
Security Provider Control Plane (SPCP)	Software	1	2	6
SPHYNX Cyber Range tool	Deployment of a novel product and service	4	6	8
ROAR tool	Deployment of a novel product and service	3	4	8
The SPHYNX Security and Privacy Assurance Suite (SPHYNX SPA Suite)	Deployment of a novel product and service	7	8	9
UEBA component of PHOENI2X	Deployment of a novel product and service	3	5	7
Honeypot	Software	3	4	5

As seen in Table 11, the current and envisioned maturity of the identified exploitable results varies. The envisioned technical maturity of the results ranges from 4 in one case to 9 for two cases.

In summary:

The current technical maturity of the identified exploitable results is: At TRL 1-2: 3, at TRL 3-4: 6, at TRL 5-6: 4 and at TRL 7-9: 1.

The envisioned technical maturity of the identified exploitable results is: At TRL 1-2: 0, at TRL 3-4: 2, at TRL 5-6: 5 and at TRL 7-9: 7.

3.3.2 Input Ranking

The CONCORDIA project[34], proposed a strategy for ranking ERs in order to derive the Key Exploitable Results of a project[35]. Based on this strategy the following criteria were identified to facilitate the ranking of the ERs.

A. Market Demand or Market Readiness Level (based on knowledge of market)

B. Innovation Potential (based on declared value proposition canvas if available, or knowledge of state of art)

C. Technical Maturity (based on declared TRL, knowledge of ER and the state of art space)

D. Network effect (why it should be done/promoted within this project instead of another EU project, OR if the ER would benefit greatly by interacting with the project community and beyond)

Each one of these criteria is measured on a scale from 1 to 5, and the ranking was performed by all partners based on the information of the ER identification documents available. The ranking of the ERs was implemented only in the cases of exploitable results of the types: Software, Service, Compliance process and Deployment of a novel product and service. The highest-ranking ERs will be named as KERs (Key Exploitable Results) and the project shall define exploitation strategies and plans for their further exploitation.

Special questionnaires were created for the ranking of the identified Exploitable results. It should be noted that the PHOENI2X solution (the solution as a whole provided by the project) is identified automatically as a Key Exploitable result and excluded from the ranking.

3.3.3 Input Ranking results

The results from the ranking implemented by the partners are the following:

Figure 31: Key Exploitable Results of the PHOENI2X project (as identified in the first iteration)

[34] https://www.concordia-h2020.eu/

[35] CONCORDIA Project. (2020, 12 30). Deliverable D5.3: 2nd year report on exploitation, dissemination and standardization. Retrieved from CONCORDIA project: https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D5.3.pdf

Following the CONCORDIA project methodology mentioned above, the ranking also provided the ERs (apart from the PHOENI2X Service / Solution) that have scored the highest per category:

e.g.

- The SANL CR, Cyber Range Tool, has been identified as the one with the highest A. Market Demand or Market Readiness Level (based on knowledge of market) and the highest D. Network effect (why it should be done/promoted within this project instead of another EU project, OR if the ER would benefit greatly by interacting with the project community and beyond).
- The SANL, UEBA Component Security analysis tool, has been identified as the one with the highest B. Innovation Potential (based on declared value proposition canvas provided in the columns to the left, or knowledge of state of art)
- The SANL, ROAR tool, has been identified as the one with the highest C. Technical Maturity (based on declared TRL, knowledge of ER and the state of art space).

Most of the ERs that have achieved the highest score in total, have also the maximum score in a specific criterion and as such, the project team decided not to change the list of KERs.

3.3.4 Analysis of Key Exploitable Results exploitation potential

Once the Key Exploitable Results have been identified, the next step in formulating the exploitation plan consists of analyzing the exploitation potential of each of the key exploitable results.

To this end, in the months September – November 2023 a preliminary analysis was conducted for each key exploitable result (the five identified in to assess their potential market opportunities, their target-audience, the market size, and the intellectual property rights (IPR) protection. The results of this analysis are summarized below:

3.3.4.1 Exploitation potential for the PHOENI2X Service / Solution

PHOENI2X holistic approach integrates Prevention, Detection & Response via a fully-featured baseline toolset. Then, AI-assisted Situational Awareness, Prediction & Response features build upon said toolset, providing enhanced and up-to-date view of the threat landscape, early warning and attack prediction capabilities, and alert and response prioritization driven by a business impact risk assessment. These can recommend and trigger specific RPs that encode, orchestrate and execute specific IR and BC processes.

These are also used to derive hands-on training covering from technical to T&A aspects, and to automatically assess the effectiveness of playbooks, facilitating their adaptation.

This process closes the feedback loop, allowing the continuous improvement of the configuration of the underlying components and the IR and BC processes themselves.

Technical maturity: The technical maturity of this exploitable result at the beginning of the project was assessed to be at the level of null (TRL0) as the solution / service was only described at a high level in the project proposal. At the end of the project, it is expected that the solution / service will be validated in a lab environment (TRL 4).

Market potential, target audience & market size: According to a report published by Market Insights in November 2023, the global cybersecurity market has witnessed a robust growth over the past few years and is expected to reach approximately US$274 billion in revenue by 2028 from US$166.20 billion in 2023. These revenues are primarily generated by its two key products, cyber solutions, and

security services, with the security services market having the largest share of the revenues. It should be noted that security services include both Managed services and professional services.

Further to this, the global Security as a Service (SECaaS) market, that was valued approximately 10.2 billion U.S. dollars in 2022, is expected to grow throughout the next years and projected to reach more than 81 billion U.S. dollars by 2033. In 2019, spending in the cybersecurity industry reached around 40.8 billion U.S. dollars. In 2022, total spending on cybersecurity technologies increased to 71.1 billion U.S. dollars, the largest amount recorded in the period under review (canalys.com, 2023). The highest increase in spending in cybersecurity was within the healthcare sector, with an annual compound growth rate of 14 percent, while the lowest growth rate was found in the sector of Aerospace and defense (European Cybersecurity Investment Platform, 2022).

When looking at the specific market of Security Orchestration, Automation and Response solutions, a VMware worldwide survey in 2022[36] provides the following insights:

Only 27,3% from the respondents have already implemented a SOAR solution. When compared to other solutions part of the survey, this represents one of the low scores (i.e., Network detection and response (NSDR) solutions are already implemented from 46,6% of the respondents).

On the other hand, 54,5% of the survey respondents will either upgrade their SOAR solution (26,1%) or acquire as new (28,4%), making SOAR one of the most needed solutions for 2022 (in comparison to the others proposed by the survey).

Figure 32 shows Technologies and solutions planned for initial use within the next 12 months, Survey of 2022, Source: Statista, VMware; ID 1331684.

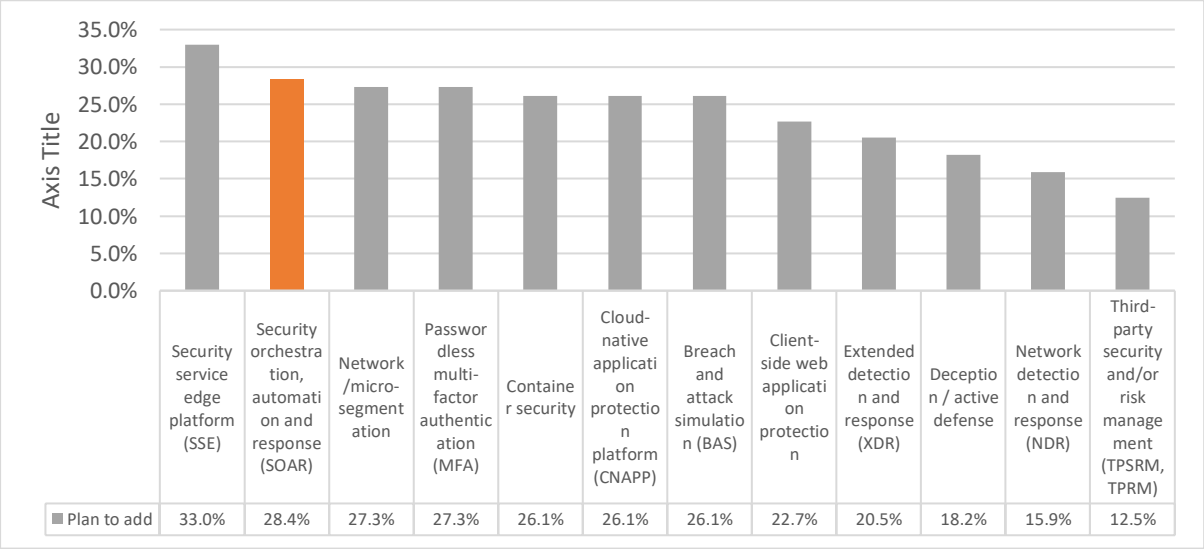


Figure 32: Technologies and solutions planned for initial use within the next 12 months, Survey of 2022, Source: Statista, VMware; ID 1331684

The market and interest for SOAR solutions is increasing. Evidence to this effect can be derived by comparing the results from the 2021 IDG Research Services worldwide services, accessible through Statista. Specifically, this survey report indicates that 37% of the respondents had SOAR "on my radar or actively searching", 12% were piloting the solution, 18% had the solution already in production and 10% were upgrading or refining.

[36] https://www.statista.com/statistics/1331684/cyber-security-technologies-in-use-upgrade-worldwide/

Finally, it should be noted that the top 7 characteristics of such solutions that appeal to the market are the following:

1st (42%) Simplified visualization of complex attacks and understanding of how they progress across a kill chain.

2nd (38%) Advanced analytics that can detect and identify modern, sophisticated attacks.

3rd (31%) Automated response capabilities that can help block attacks in progress.

4th (31%) Improvement of mean time to detect and/or mean time to respond.

5th (30%) Aggregation and correlation of security data from multiple security controls and sources.

6th (26%) Consolidation of multiple security tools into a single threat detection and response solution.

7th (25%) Prioritization of security incidents / alerts based upon the severity of attack.

The source of the above information is Symantec, ESG and is accessible through Statista.

Major players: The Security Orchestration Automation and Response (SOAR) market is highly competitive, with several major players dominating the industry. IBM, FireEye, Cisco Systems, Rapid7, Splunk, Swimlane LLC, Tufin, ThreatConnect, Demisto (Palo Alto Networks), DFLabs, LogRhythm, Siemplify, Resolve Systems, CyberSponse, and Exabeam are some of the key companies in this market.[37]

Intellectual Property Rights (IPR) Protection: The issue of IPR protection should be considered, taking also into consideration that the PHOENI2X Service / Solution, comprises from a number of components, the majority of which (as shown below) are owned by the partners of the project.

3.3.4.2 ROAR Incident Response tool – SANL exploitation potential

ROAR, which builds upon the SPHYNX Incident Response tool, offers a security orchestration, automation, and response (SOAR) solution supporting the prevention, detection, investigation, and response to cyber security attacks. To do so, the tool uses executable playbooks specified according to the OASIS CACAO standard.

Technical maturity: The technical maturity of this exploitable result at the beginning of the project was assessed to be at the level of experimental proof of concept (TRL3). At the end of the project, it is expected that the system will be complete and qualified (TRL8).

Market potential, target audience & market size: The information regarding this section, is mentioned in 3.3.4.1Exploitation potential for the PHOENI2X Service / Solution.

Major players: Some of the key players in the Cybersecurity market are Microsoft, IBM, Cisco, Paloalto networks, Fortinet, Crowdstrike, and Capgemini.

Intellectual Property Rights (IPR) Protection: Several patents and/or patent applications have been found that are similar to ROAR, such as:

1. **Proactive Anti Cyber-Forensic Activity Detection and Prevention (US2023342455 (A1))**

   Computer-implemented cyber-security processes and machines provide proactive anti-forensics activity detection and prevention to safeguard the integrity of transactions and their associated log details or other data using artificial intelligence and/or machine learning,

[37] https://www.linkedin.com/pulse/security-orchestration-automation-response-soar-market-insights-dsv6f/

thereby ensuring that all transactions and logs within the system are complaint for cyber forensics, and helping to make reactive forensic tasks more robust by adding proactive monitoring and compliance activity.

2. **System and Method for Surfacing Cyber-Security Threats with a Self-Learning Recommendation Engine (US2023336586 (A1))**

   Techniques for performing cyber-security alert analysis and prioritization according to machine learning employing a predictive model to implement a self-learning feedback loop. The system implements a method generating the predictive model associated with alert classifications and/or actions which automatically generated, or manually selected by cyber-security analysts. The predictive model is used to determine a priority for display to the cyber-security analyst and to obtain the input of the cyber-security analyst to improve the predictive model. Thereby the method implements a self-learning feedback loop to receive cyber-security alerts and mitigate the cyberthreats represented in the cybersecurity alerts.

3. **Cyber security platform and method (US11736497)**

   A method of providing cyber security to an industrial control system is described. The method includes detecting an anomaly and recording and reporting the detected anomaly to a control system within a network associated with the industrial control system. Detecting the anomaly may include recording all unauthorized attempts to connect to a communication port in the network, capturing identifying information associated with the unauthorized attempts, detecting scanning activity of a hacker in the network, detecting an attempt to manipulate a log file to conceal malicious activity in the network; and recording and reporting the detected anomaly to a controller within the network.

As businesses continuously migrate their data to the cloud and improve their information technology infrastructure, the related threats to their data also increase. For this reason, security solutions are high in demand to ensure data security. The increasing number of cyber-attacks, due in part to the pandemic-driven shift from offline to online activities, is prompting more and more companies to invest in cyber security services, and solutions, resulting in a thriving zero-trust security market. Taken together with the advancements in artificial intelligence, and machine learning, and the evolution of Internet of Things, the zero-trust model is expected to drive the future evolution of the cyber security market. The above suggest that ROAR has significant market potential, that could be exploited once the product has been fully developed, and its intellectual property rights have been adequately protected through a patent or any other appropriate protection method. However, given that the market is highly dominated by major players, competition is expected to be particularly high.

3.3.4.3 CR Cyber Range tool – SANL

The SPHYNX Cyber Range tool offers cyber security training that covers a comprehensive spectrum of known and emerging security and privacy threats and is tailored to the particular security and privacy risks of different organizations.

Technical maturity: The technical maturity of this exploitable result at the beginning of the project was assessed as being at the level of technology validated in lab (TRL4). At the end of the project, it is expected that the product will be complete and qualified (TRL8).

Market potential, target audience & market size: E-mail fraud (business e-mail compromise), smishing/vishing, and ransomware attacks, have been identified as some of the most significant cybersecurity threats in organizations worldwide (Proofpoint, 2023). To address these threats, companies have started implementing security awareness training programs in topics such as password best practices, email-based phishing, malware, wi-fi security, ransomware, mobile device security, cloud-based threats, and so on (Proofpoint, 2022). In 2022, when asked about cybersecurity investments planned by their companies, over 50 percent of respondents from the United States

stated that their organization was planning to invest in employee security awareness training (Keeper Security, 2022). In these security awareness programs, companies have used several tools, ranging from in-person training sessions, and virtual instructor-led training, to computer-based training, simulated phishing attacks, and smishing and/or vishing simulations (Proofpoint, 2022). Of these tools, computer-based training was identified as being the most popular (Proofpoint, 2022).

Major players: Some of the top Cybersecurity Education and Training Providers are Digital Defense Inc., KnowBe4, Inspired eLearning, Security University, Infosec Institute, SecureNinja, Concise Courses, VigiTrust, Blackfin, and (ISC)2. Some of the companies managing cyber ranges are: Cloud Range, Cyber Ranges, Cyberbit, Cyrin, Field Effect, IBM, RangeForce, Tech Data, U.S. Cyber Range. In Europe, some of the cyber range providers are: Airbus CyberRange, AIT Cyber Range, AMOSSYS Cyber Range, CDEX, Paideusis, CITEF, Coliseum, CYS4 – SOC CyberRange, CybExer Cyber Range Platform, Cyber Range Laboratory, Cyber Trainer, Diateam HNS, hackrocks, NCR (Norwegian Cyber Range), Realistic Global Cyber Environment (RGCE), WithSecure Playground, DETER/DeterLab, EDU Range, KYPO Cyber Range, UNIGE CRACK Multidomain CyberRange (CRACK MCR). The list of European cyber ranges is published in the publication of ECSO WG5, 2022 Edition "CYBER RANGE FEATURES CHECKLIST & LIST OF EUROPEAN PROVIDERS"[38].

Intellectual Property Rights (IPR) Protection: Given the plethora of similar cyber security training programs, the SPHYNX Cyber Range tool cannot be considered patentable. It could be protected, however, through copyright, or patented as part of a broader cybersecurity system and tool.

Taken together, the above suggest that the SPHYNX Cyber Range tool has significant market potential, that could be exploited once the product has been fully developed. However, the market is highly competitive, with several players having a significant share of the market. This suggests that significant efforts should be made to develop and highlight the competitive advantage and unique selling point of the specific tool.

3.3.4.4 TINTED CTI Discovery, Analytics & Threat Hunting (TII) – ATOS

TINTED aims to address the challenges faced by security analysts when analyzing large volumes of security events coming from external sources. It scores events, allowing filtering of non-relevant events and analyst to focus on high-scored and relevant events. These capabilities save time, improve the protection capabilities, and save costs for the company. Other functionalities support fine grained data sharing, and automation of attack prevention actions.

Technical maturity: At the start of the project, the technical maturity of this software was at the level of the experimental proof of concept (TRL3). At the end of the project, it is expected that the software will be validated in the lab (TRL4).

Market potential, target audience and market size: The market for security event analysis tools is highly competitive and fragmented, with over 50 SIEM solutions available. According to Market Research Future (2023), the Information Security and Event Management (SIEM) Market is growing at a CAGR of 7.90% for the period 2022 to 2030 with US$ value of 6.77 billion. The latest trends suggest that there will be a significant rise in the market in the coming years (Market Research Future, 2023). The global market recorded a net valuation of US$ 1.75 billion in the year 2017. The current projections show that the market is growing at a CAGR of 14.6% for the forecast period of 2020 to 2027, while the estimated market value will reach US$ 3.89 billion by the end of 2027. Presently the gross profit of SIEM services is limited to large-scale enterprises. A huge number of SMEs in developing

[38] https://mcusercontent.com/dd08496e1863c5ea11d77abac/files/533dbacf-d122-aff5-bc11-ec1bdedbb0d5/Cyber_Range_Features_Checklist_List_of_European_Providers_v1_final.01.pdf

countries can be a potential market for software services in the future. To accelerate their reach to the end-users, large technological companies form strategic partnerships, and corporate mergers and acquisitions.

Major players: The biggest key players in the global security information and event management market are Hewlett Packard Enterprise (US), IBM Corporation (US), McAfee LLC (US), TrendMIcro Inc (Japan), Assuria Ltd (UK), Dell EMC (US), Logrhythm Inc (US), LogPoint A/S (Denmark), AlienVault Inc (US). Top threat intelligence tools are[39]: Anomali ThreatStream, IBM X-Force Exchange, IntSights Threat Intelligence Platform, LookingGlass Cyber Solutions, Recorded Future, SolarWinds Security Event Manager, ThreatConnect, MISP, ManageEngine Log360, Datadog Security Monitoring, Logpoint SIEM, SolarWinds Security Event Manager and Splunk Enterprise Security (comparitech.com, 2023).

Intellectual Property Rights (IPR) Protection: Due to the plethora of similar SIEM tools, such as ManageEngine Log360, Datadog Security Monitoring, Logpoint SIEM, SolarWinds Security Event Manager Splunk Enterprise Security (comparitech.com, 2023), TINTED cannot be considered as patented. It could be protected, however, through copyright, or patented as part of a broader cybersecurity system and tool.

Taken together, the above suggests that TINTED has significant market potential, that could be exploited once the product has been fully developed. However, the market is highly competitive, with several players having a significant share of the market. This suggests that significant efforts should be made to develop and highlight the competitive advantage and unique selling point of the specific tool.

3.3.4.5 CP Compliance Process – NCSA

The CP compliance process aims to raise entities' awareness and compliance level, regarding NIS2 requirements on Incident alerting and reporting.

Technical maturity: At the start of the project, the technical maturity of the CP Compliance Process was assessed to be at the level of "basic principles observed" (TRL1). At the end of the project, it is expected that the process will be validated in a relevant environment (TRL6).

Market potential, target audience and market size: The CP Compliance Process belongs to the broad professional cybersecurity services market, which are a set of specialized services that include a broad range of areas, such as incident response, threat intelligence, compliance management, security architecture and design, computer forensics and investigations, security awareness and training, and cybersecurity strategy (Statista.com, 2023). According to Statista Market Insights (2023), the total revenues of this market reached US$ 64.77 billion, and they are expected to reach US$ 88.03 billion in 2028. Furthermore, the average spend in these professional services per employee shows a steadily increasing trend from US$ 18.60 in 2023 to a projected US$ 24.62 in 2028, following the growing trend of the global spending on information security products and services that is expected to reach almost US$ 300 billion in 2030 from US$ 219 billion in 2023 (IDC, 2023). The leading region in terms of generated revenues in the United States (U.S.), with US$ 30,290 million, followed by the United Kingdom (US$ 3,940 million), Japan (US$ 3,891 million), China (US$ 3,056 million), and Germany (US$ 2,607 million).

Major players: This is a tailored service that could be integrated in the operations of the Hellenic National Cyber Security authority and can not be compared to others.

[39] https://www.esecurityplanet.com/products/threat-intelligence-platforms/

Intellectual Property Rights (IPR) Protection: Due to the nature of the service, the CP compliance process cannot be considered as patentable.

3.3.5 Exploitation plan

Driven by the pandemic-led shift from offline to online activities, the increasing digitalization of modern organizations, the advances in artificial intelligence and machine learning, the evolution of the Internet of Things, and most importantly the increasing number of cyberattacks, the global cybersecurity market has witnessed a robust growth over the past few years, and is expected to continue to grow in the years to come, especially in regions such as the United States. Within this market, the security services market within which the project's processes, systems and tools belong, is also expected to grow. However, the landscape is highly competitive, as the market is dominated by very large corporations, such as Palo alto, IBM, Solar winds and others as indicated above, leaving little room for smaller players to enter.

To harness the identified market potential of the PHOENI2X Service / Solution, while addressing the inherent challenges, the following actions are planned to be executed as part of the planning for the PHOENI2X Service / Solution exploitation plan:

A. Allocation of ownership rights among partners

Before discussions can occur regarding the commercialization of the PHOENI2X Service / Solution, its accompanying processes and tools, the allocation of the ownership rights among the project partners should be varied out. As mentioned above, the PHOENI2X Service / Solution is a consolidation of different tools, services and solutions coming from the different partners.

B. Intellectual property rights strategy

After the ownership has been clarified, the second step consists in selecting the appropriate intellectual property rights strategy. To this end:

(1) a preliminary search can be conducted to assess the state-of-the-art in the specific domain by searching relevant patent databases, such as espacenet, etc.

(2) In case the developed solution differs significantly from other patented products, a cost-benefit analysis should be conducted, and a decision should be made whether an application for a patent (national, PCT, unitary patent, etc.) should be filed.

(3) If a patent application process is initiated, all project partners should refrain from any publications of the result results until the application is submitted. At the same time, several issues pertaining to the patent application process should be clarified among the partners, such as (a) who will be the applicant, (b) how will decisions be made, (c) how will the costs pertaining to the filling of the patent and the maintenance fees be covered.

(4) If the service / solution is identified as non-patentable, then suitable actions should be implemented to identify the IPR for each part of the solution / service and identify any constraints regarding future commercialization steps.

D. Development of appropriate commercialization strategy

A decision should also be made regarding the appropriate commercialization strategy. The most common commercialization strategies are:

1. ***Licensing***: Licensing is a common strategy for commercializing research results. In this approach, a company or individual pays for the right to use the intellectual property

developed by the research team. This can be a lucrative option for researchers who do not have the resources to bring their products to market themselves.

2. ***Joint venture***: Joint ventures involve partnering with an existing company to commercialize research results. This approach is ideal for researchers who want to leverage the expertise and resources of an established company to bring their products to market.
3. ***Patent sales***: Patent sales involve selling the intellectual property developed by the researcher or research team to another company or individual. This can be a lucrative option for researchers who do not have the resources to bring their products to market themselves.
4. ***Creation of spin-off or start-up****:* Spin-offs or start-ups are new companies that are created to commercialize research results. This approach is ideal for researchers who want to retain control over the commercialization process and who have the resources to start a new company.

   Under this option, the company can adopt different revenue models, such as:

   a) Subscription-based model: In this model, customers pay a recurring fee for access to cybersecurity services. This model is popular among small and medium-sized businesses that require ongoing protection against cyber threats.

   b) Pay-per-use model: In this model, customers pay for cybersecurity services on a per-use basis. This model is ideal for businesses that require occasional or one-time protection against cyber threats.

   c) Freemium model: In this model, customers can access basic cybersecurity services for free, but must pay for premium features. This model is popular among consumers and small businesses.

   d) Managed services model: In this model, cybersecurity service providers manage all aspects of a customer's cybersecurity needs, including monitoring, threat detection, and incident response. This model is popular among large enterprises that require comprehensive cybersecurity solutions.

   e) Consulting model: In this model, cybersecurity service providers offer consulting services to help businesses identify and mitigate cyber risks. This model is popular among businesses that require expert advice on cybersecurity matters.

   f) Product sales model: In this model, cybersecurity service providers sell hardware or software products that help businesses protect against cyber threats. This model is popular among businesses that prefer to manage their own cybersecurity needs.

The steps described above and the options presented shall be evaluated during the next months, in order to be in a position to extract the relevant decisions until the end of the project.

Furthermore, since some of the KERs are expected to reach an acceptable maturity during the next months, Task 6.2 will collaborate with Task 6.3 and the relevant involved partners in order to gain further insights and interaction with stakeholders.

3.4 Innovation management

As it has been stated under D1.2, PHOENI2X has established an initial innovation plan describing activities divided in RP1 and RP2. Regarding RP1 the planned activities are showcased in the table below.

Table 12 RP1 planning activities

Period		**Objectives / Actions**
RP1	M1-M18	IMT (working group) set-up
		IMT regular meetings
		IPR Register definition
		KPIs definition
		Innovations monitoring
		Innovation Radar Questionnaire v1
		Contributions to Periodic Report 1

The IMT has been shaped by the coordinator and it consists of the Innovation manager (IM) which is responsible for the monitoring of the above activities and the WP leaders. Regular meetings have been set, every first Tuesday of each month.

Over the last period the IMT with the assistance of the rest of the consortium defined the innovation to be developed within the framework of PHOENI2X. Partners with the assistance of WSE and APS, filled in the below table which gives the whole picture of each individual innovation.

Table 13 Partners individual innovation

Partner	***Product***	***Technological Areas***	***Market***	***Innovation ID***	***Technical ExtensionID***	***Innovation Name***	***Description***
UPAT	Deception Tools (Honey pots)	Honeypot	IDS (Intrusion Detection System)	ID1	UPAT.PE01	DLMS COSEM Honeypot	Extension current product
AEGIS	Digital Forensics (FVT)	Digital forensics investigation, Digital evidence analysis, Big Data vizualisation	Digital Forensics	ID2	AEGIS.PE01	Forensics Visualization Toolkit (FVT)	Extension current product
SANL	Security Assurance Platform	SIEM, Vulnerability Assessment, Risk Assessment	Integrated Risk Management	ID3	SANL.PE01	SPHYNX SPA Suite	An integrated suite of tools that provides comprehensive cyber security risk detection and management for enterprise systems
SANL	Cyber Range (CR)	Cyber Range Training	Security Training & Awareness	ID4	SANL.PE02	SPHYNX Cyber Range Tool	A tool for the delivery of cyber range exercises for different assets (and combinations of assets) of an organisation, and particular types of security and privacy threats, vulnerabilities,

							and risks identified for them.
SEA	Serious Games - HATCH	Serious Game (tabletop)	Requirement Elicitation, Awareness raising and training	ID5	SEA.PE01	New Scenarios	Extension current product (new scenarios)
SEA	Serious Games - PROTECT	Serious Game (software)	Awareness raising and training	ID6	SEA.PE02	New content	Extension current product (new content) and slightly improved maturity
SEA	Serious Games – CyberSecurity Awareness Quiz	Serious Game (software)	Awareness raising and training	ID7	SEA.PE03	AI assistance	New function (automatic content generation) and improved maturity
SANL	ROAR	Incident Response	Security Orchestration, Automation & Response	ID8	SANL.PE03	SPHYNX Incident Response tool	A SOAR solution supporting the prevention, detection, investigation, and response to cyber security attacks, via CACAO-based playbooks.
ATOS	Risk Impact Assessment & Prioritisation (CERCA)	Risk Management	Integrated Risk Management	ID9	ATOS.PE01	New Scenarios and features	- Definition of new models for UCs representing the threat landscape. - Extension of the tool with new indicators. - Prioritization of mitigation actions.
UPC	Attack Pred., Resp. Recom. & Adaptation (PMEM)	Attack prediciton and detection	IDS (Intrusion Detection System)	ID10	UPC.PE01	New models	Extension of current product.
ATOS	CTI Discovery, Analytics & Threat Hunting (TII)	Threat intelligence	Threat intelligence	ID11	ATOS.PE02	TI Analytics Improvement	Classification of the events per sectors. Automated prevention with CACAO and OpenC2.

SANL	UEBA	Security ML-based Analytics	Threat Detection & Analytics	ID12	SANL.PE03	SPHYNX Security Analytics Tool	ML-based analysis of raw events and security assessments based on classification and prediction algorithms that provide different types of user and entity behaviour analysis (UEBA) profiles.
ATOS	Alerting, Rep. & Info. Ex. Engine (SMIR)	Incident Reporting	Incident Response	ID13	ATOS.PE03	New Regulations and Response Automations	Inclussion of new regulations and new workflows. New automations on reporting via email.

As the project is getting into a more mature period where advancements on the development of the innovations and implementation are going to take place, it is planned to follow the innovation radar procedures. For this reason, during the RP2, PHOENI2X will classify the innovations listed above in terms of maturity (market, tech, business ready or exploring) and inform the PO for initiating the process of including the selected innovation into the EU innovation radar. In parallel, a release of Open Data and the alignment with the exploitation team will take place.

In a nutshell, the activities of the IMT for RP2 are show at the below table.

Table 14 RP2 planning activities

Period		**Objectives / Actions**
RP2	M19-M36	Innovation Radar process initiation
		IMT regular meetings
		IPR Register maintenance
		Innovations monitoring
		Alignment with Exploitation team
		Release of Open Data (ZENODO)
		Final IPR Report

4 STANDARDIZATION

4.1 What is standardisation[40]?

A standard is a document that sets the technical requirements of a product, service or process and its use. Standards are adopted by recognised standardisation bodies (such as ISO, CEN, CENELEC, ETSI, and many more). In these organisations, representatives from industry, research, governments and civil society, discuss and agree on what should be a standard. Once a standard is published, its use is normally voluntary but, in some cases, certain specific standards can be made mandatory by law. In other words, standards form a common language that allows researchers, people, public institutions and industry to communicate, produce and commercialise products and services in a harmonised manner. This is especially important in the European single market.

Standards play an important role in the valorisation of research & innovation results[41]:

- They help researchers bring their innovation to the market and spread technological advances by making their results transparent. In spreading the diffusion of new technologies, standards provide both economic opportunities, facilitate realisation of SDGs and give confidence to consumers that an innovative technology is safe. They codify the technology requirements and inform both manufacturers and consumers on what to expect.
- They allow technologies and materials to be interoperable: since a standard provides details on the use and content of a technology or a material, it is much easier to know when and how it can be used in combination with other technologies.
- In other words, by codifying information on the state of the art of a particular technology, standards enable dissemination of knowledge (both within and outside the relevant industry community). Moreover, standards bridge the gap between research and products or services allowing the diffusion of the technology in the market and increasing the probabilities of its take-up. Standardisation facilitates the deployment of new technologies, interoperability between new products and services. Innovations can more easily gain market acceptance and consumer trust if they comply with existing standards for safety, quality, performance and sustainability.

4.2 PHOENI2X standardization strategy

From the beginning of the project, the members of the project, identified the key topics of the PHOENI2X project and searched for 1) possible standards that can be of use to the project and 2) possible standardization efforts where the project could provide useful contribution.

The main topics identified for the project where:

- Cyber Resilience
- Cyber security tools using Artificial intelligence
- Security orchestration, automation & response
- Business continuity and recovery
- Incident response

[40] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf
[41] https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/eu-valorisation-policy_en

- Information Exchange
- Cybersecurity related directives and acts of the European Union
- Practical Cybersecurity training
- Simulation
- Cybersecurity attacks
- Preparedness

The Standards Developing Organizations identified having developments on the above topics are:

ETSI

ETSI is a European Standards Organization (ESO). It is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.

ETSI has a special role in Europe. This includes supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

ETSI is structured in technical committees, one of which is ETSI CYBER (TECHNICAL COMMITTEE (TC) CYBER (CYBERSECURITY))[42].

ETSI TC CYBER is recognized as a major trusted centre of expertise offering market-driven cybersecurity standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. We provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques. TC CYBER is the most security-focused technical committee in ETSI.[43]

There are too many publications of ETSI TC CYBER, so it is not possible to present them here. Instead, some were selected and are showcased below, as an example of standards having relevance to this project:

ETSI TR 103 303 V1.1.1 (2016-04)[44]: Protection measures for ICT in the context of Critical Infrastructure.

ETSI TR 103 331 V1.1.1 (2016-08)[45]: Structured threat information sharing.

ETSI GR SAI 004 V1.1.1 (2020-12)[46]: Securing Artificial Intelligence (SAI). Problem Statement.

ETSI TR 103 456 V1.1.1 (2017-10)[47]: Implementation of the Network and Information Security (NIS) Directive.

ETSI TR 103 866 V1.1.1 (2023-02)[48]: Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls.

[42] https://www.etsi.org/committee/cyber
[43] https://www.etsi.org/cyber-security/tc-cyber-roadmap
[44] https://www.etsi.org/deliver/etsi_tr/103300_103399/103303/01.01.01_60/tr_103303v010101p.pdf
[45] https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.01.01_60/tr_103331v010101p.pdf
[46] https://www.etsi.org/deliver/etsi_gr/SAI/001_099/004/01.01.01_60/gr_SAI004v010101p.pdf
[47] https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
[48] https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf

ETSI TR 103 331 V2.1.1 (2022-12)[49]: Structured threat information sharing.

ETSI GS ISI 004 V1.1.1 (2013-12)[50]: Information Security Indicators (ISI). Guidelines for event detection implementation.

ETSI GS ISI 002 V1.2.1 (2015-11)[51]: Information Security Indicators (ISI). Event Model. A security event classification model and taxonomy
ETSI GS ISI 003 V1.2.1 (2018-01)[52]: Information Security Indicators (ISI). Key Performance Security Indicators (KPSI). to evaluate the maturity of security event detection

CEN/CENELEC[53]

CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries.

CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes.

CEN supports standardization activities in relation to a wide range of fields and sectors including: air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CENELEC, the European Committee for Electrotechnical Standardization, is an association that brings together the National Electrotechnical Committees of 34 European countries

CENELEC prepares voluntary standards in the electrotechnical field, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.

CENELEC supports standardization activities in relation to a wide range of fields and sectors including: Electromagnetic compatibility, Accumulators, primary cells and primary batteries, Insulated wire and cable, Electrical equipment and apparatus, Electronic, electromechanical and electrotechnical supplies, Electric motors and transformers, Lighting equipment and electric lamps, Low Voltage electrical installations material, Electric vehicles railways, smart grid, smart metering, solar (photovoltaic) electricity systems, etc.

CEN/CENELEC is also organized in Technical Committees. CEN/CLC/JTC 13 is the committee covering the topics Cybersecurity and Data Protection.

There are too many publications of CEN/CLC/JTC 13, so it is not possible to present them here. Instead, some were selected and are showcased below, as an example of standards having relevance to this project:

CEN/CLC/TS 17880:2022 (2022-12)[54]: Protection Profile for Smart Meter - Minimum Security requirements.

[49] https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/02.01.01_60/tr_103331v020101p.pdf
[50] https://www.etsi.org/deliver/etsi_gs/ISI/001_099/004/01.01.01_60/gs_ISI004v010101p.pdf
[51] https://www.etsi.org/deliver/etsi_gs/ISI/001_099/002/01.02.01_60/gs_ISI002v010201p.pdf
[52] https://www.etsi.org/deliver/etsi_gs/ISI/001_099/003/01.02.01_60/gs_ISI003v010201p.pdf
[53] https://www.cencenelec.eu/about-cen/
[54]https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:73956,2307986&cs=153E4E09D0E271F65197F2461D0548660

EN ISO/IEC 27001:2023 (2023-7)[55]: Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022).

EN ISO/IEC 27041:2016 (2016-8)[56]: Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015).

EN ISO/IEC 27043:2016 (2016-8)[57]: Information technology - Security techniques - Incident investigation principles and processes (ISO/IEC 27043:2015).

[Under Development] prEN XXX[58]: Managed Security Services Providers Requirements. This standard defines requirement areas which are of relevance for the quality of a managed security service and map the specific requirements to different types of services in scope. For every type of service in scope there needs to be a clear definition of what is required to justify a certain level of security claim.

ISO[59]

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 169 national standards bodies.

Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

ISO is also organized in Technical Committees.

ISO/IEC JTC 1/SC 27 is the committee covering the topics Information security, cybersecurity and privacy protection.

SC 27[60] develops standards in the field of information security, cybersecurity and privacy protection, through its five working groups:

- WG 1 – Information security management systems
- WG 2 – Cryptography and Security Mechanisms
- WG 3 – Security Evaluation, Testing and Specification
- WG 4 – Security Controls and Services
- WG 5 – Identity Management and Privacy Technologies

SC 27 membership includes approximately 81 countries.

There are too many publications of ISO/IEC JTC 1/SC 27, so it is not possible to present them here. Instead, some were selected and are showcased below, as an example of standards having relevance to this project:

[55] https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:77035,2307986&cs=1BFADC8AE3DA7047F3F09769CAFC93E48
[56] https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61348,2307986&cs=1D05CB5B99C541AD26D674C795C1C4BB3
[57] https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61350,2307986&cs=1A8926672B7DC205570410E1ADA81CD38
[58] https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:71231,2307986&cs=10265E080B5342B0A820C5762FCEDBB5F
[59] https://www.iso.org/about-us.html
[60] https://committee.iso.org/home/jtc1sc27

ISO/IEC 27031:2011 (2011-03)[61]: Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

[Under Development] ISO/IEC DIS 27031[62]: Information and communication technology readiness for business continuity. This document describes the concepts and principles of information and communication technology (ICT) readiness for business continuity (IRBC). It provides a framework of methods and processes to identify and specify aspects for improving an organization's ICT readiness to ensure business continuity. This document serves the following business continuity objectives for ICT: Maximum Tolerable Period of Disruption (MTPD), Recovery Point Objective (RPO), Recovery Time Objective (RTO) as part of the ICT Business Continuity Planning. This document applies to all types and sizes of organizations. This document describes how the ICT department plan and prepare to contribute to the resilience objectives desired by the organization.

ISO/IEC 27035-1:2023 (2023-02)[63]: Information technology. Information security incident management. Part 1: Principles and process.

ISO/IEC 27035-2:2023 (2023-02)[64]: Information technology. Information security incident management. Part 2: Guidelines to plan and prepare for incident response.

ISO/IEC 27035-3:2020 (2020-09)[65]: Information technology. Information security incident management. Part 3: Guidelines for ICT incident response operations.

[Under Development] ISO/IEC DIS 27035-4[66]: Information technology. Information security incident management. Part 4: Coordination. This document provides the guidelines for coordination among multiple organizations to work together to handle information security incidents. It also addresses the impacts of external cooperation to the internal incident management of an individual organization, and provides guidelines for an individual organization to adapt to the coordination. Furthermore, it provides guidelines for the coordination team, if it exists, to perform coordination activities supporting the cross-organization incident response.

ISO/IEC 27041:2015 (2015-06)[67]: Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method.

ISO/IEC 30111:2019 (2019-10)[68]: Information technology. Security techniques. Vulnerability handling processes.

ISO/TC 292 is the committee covering the topics Security and resilience.

The mission for ISO/TC 292[69] Security and resilience is to produce high quality standards to support nations, societies, industry, organisations and people in general. The purpose of these standards is to enhance and sustain the state of being free from danger or threat and to feel safe, stable, and free from fear or anxiety. ISO/TC 292 was established on January 1 in 2015 and is a committee with over 50 involved countries. It works with standardization in the field of security to enhance the safety and

[61] https://www.iso.org/standard/44374.html
[62] https://www.iso.org/standard/80975.html
[63] https://www.iso.org/standard/78973.html
[64] https://www.iso.org/standard/78974.html
[65] https://www.iso.org/standard/74033.html
[66] https://www.iso.org/standard/80975.html
[67] https://www.iso.org/standard/44405.html
[68] https://www.iso.org/standard/69725.html
[69] https://www.isotc292online.org/

resilience of society. The committee is responsible for more than 20 published International Standards.

There are too many publications of ISO/TC 292, so it is not possible to present them here. Instead, some were selected and are showcased below, as an example of standards having relevance to this project:

ISO 22300:2021 (2021-02)[70]: Security and resilience. Vocabulary

ISO 22301:2019 (2019-10)[71]: Security and resilience. Business continuity management systems. Requirements.

ISO 22313:2020 (2010-02)[72]: Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301.

ISO 22317:2021 (2021-11)[73]: Security and resilience. Business continuity management systems. Guidelines for business impact analysis

ISO 22320:2018 (2018-11)[74]: Security and resilience. Emergency management. Guidelines for incident management.

ISO/TS 22332:2021 (2021-05)[75]: Security and resilience. Business continuity management systems. Guidelines for developing business continuity plans and procedures.

ISO/TR 22351:2015 (2015-09)[76]: Societal security. Emergency management. Message structure for exchange of information.

OASIS[77]

One of the most respected, non-profit standards bodies in the world, OASIS Open offers projects—including open source projects—a path to standardization and de jure approval for reference in international policy and procurement.

People join OASIS to advance projects for cybersecurity, blockchain, IoT, emergency management, cloud computing, legal data exchange, and much more. The technologies vary, but our mission stays the same: to advance the fair, transparent development of open source software and standards through the power of global collaboration and community.

OASIS Open offers four key programs to support and amplify work.

Technical Committees. Develop specifications in an open, lightweight process with a path to recognition in international policy and procurement—with both integrity and rapid progress.

Open Projects. Work in an environment of cross-organizational sharing and collaboration, where you can develop open source code and standards, too.

[70] https://www.iso.org/standard/77008.html
[71] https://www.iso.org/standard/75106.html
[72] https://www.iso.org/standard/75107.html
[73] https://www.iso.org/standard/79000.html
[74] https://www.iso.org/standard/67851.html
[75] https://www.iso.org/standard/50069.html
[76] https://www.iso.org/standard/57384.html
[77] https://www.oasis-open.org/org/

Foundation-as-a-Service. Get the infrastructure and fiscal agency services to quickly form and run an independent foundation.

Technical Advisory Groups to ISO. Represent U.S. interests in global standards produced by ISO.

CACAO: Collaborative Automated Course of Action Operations for Cyber Security[78]

CACAO TC members are developing a standard to implement the course of action playbook model for cybersecurity operations.

In order to defend against cyber threats, organizations must manually identify, create, and document the prevention, mitigation, and remediation steps that, together, form a course of action playbook. However, today, there is is no standardized way to document and share these playbooks across organizational boundaries and technology solutions.

CACAO addresses this problem by defining a sequence of cyber defense actions that can be executed for each type of playbook. It will specifically enable organizations to:

- create course of action playbooks in a structured machine-readable format,
- digitally sign course of action playbooks,
- securely share course of action playbooks across organizational boundaries and technological solutions, and
- document processing instructions for course of action playbooks in a machine readable format.

Currently published standards include:

CACAO Security Playbooks Version 1.0. (2023-06)[79]: Edited by Bret Jordan and Allan Thomson. 23 June 2021. OASIS Committee Specification 02.

CACAO Security Playbooks Version 1.0. (2021-01)[80]: Edited by Bret Jordan and Allan Thomson. 12 January 2021. OASIS Committee Specification 01.

TC Work In Progress : Security Playbook Requirements & Security Playbook Specification.

OASIS Cyber Threat Intelligence (CTI) TC[81]

The OASIS Cyber Threat Intelligence (CTI) TC was chartered to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. The CTI TC focuses on development and standardization of STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information) under the OASIS open standards process.

The OASIS CTI Technical Committee will:

- define composable information sharing services for peer-to-peer, hub-and-spoke, and source subscriber threat intelligence sharing models

[78] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao
[79] https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html.
[80] https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html
[81] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

- develop standardized representations for campaigns, threat actors, incidents, tactics techniques and procedures (TTPs), indicators, exploit targets, observables, and courses of action
- develop formal models that allow organizations to develop their own standards-based sharing architectures to meet specific needs

Currently published standards include:

- STIX v2.1 OASIS Standard
- TAXII v2.1 OASIS Standard
- STIX v2.1 Interoperability Test Document Version 1.0
- TAXII v2.1 Interoperability Test Document Version 1.0

The project partners, are monitoring the various Standard Developing Organizations and efforts, and when suitable to the context of the PHOENI2X project standardization efforts are identified, activities will be carried out in order to contribute.

4.3 PHOENI2X standardization activities

4.3.1 ISO/IEC 27017[82]

A member of the partner organization APS is participating in the development of the ISO/IEC 27017 standard as co-editor.

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;

- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

The current development stage of the standard is CD (Committee study initiated).

4.3.2 CEN/CLC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"

CEN/CLC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act" is a s special working group created under CEN/CLC/JTC 13[83].

The purpose of the working group was to provide information and complement activities related to the Cyber Resilience act (CRA).

APS, a partner of the PHOENI2X project, is a member of this working group and works on providing feedback on the relevant requests and assignments. The CRA is of importance and relevance to the PHOENI2X project since it relates and defines actions and requirements in relation to the following objectives[84]:

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

[82] https://www.iso.org/standard/82878.html
[83] https://www.din.de/en/getting-involved/standards-committees/nia/european-committees
[84] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives were set out:

- ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
- ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
- enhance the transparency of security properties of products with digital elements, and
- enable businesses and consumers to use products with digital elements securely.

4.3.3 CEN / CENELEC CWA 18028[85] / 18024[86] / 18023[87]

CEN / CENELEC CWA 18028

CEN Workshop Agreement (CWA 18028:2023) has been developed in accordance with the CEN/CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2023-07-09, the constitution of which was supported by CEN following the public call for participation made on 2022-02-15. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

This document specifies a formal definition of a semantic layer that contains the list of field names to be used in the messages transmitted during a crisis.

Additionally, the document evaluates the suitability of the following standards:

— OASIS EDXL-CAP [6] for automatically collecting part of the information of a crisis involving critical infrastructures; and

— OASIS EDXL-SitRep [7] for the generation of situation reports from the information collected in the system and their automatic delivery to the strategic command.

The standard has reached the CWA stage. Further activities regarding the future of this standard have not been released yet.

The partners ATOS and APS of the PHOENI2X project have been involved in the development of this standard.

CEN / CENELEC CWA 18024

This CEN Workshop Agreement (CWA 18023:2023) has been developed in accordance with the CEN/CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2023-07-05, the constitution of

[85] https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa18028.pdf
[86] https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa18024.pdf
[87] https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa18023_2023.pdf

which was supported by CEN following the public call for participation made on 2022-02-15. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2023-07-24.

This document provides requirements and recommendations for a common set of information, datatypes and terms to be reported and provided by affected critical infrastructures to national or local coordination centres or control rooms of emergency services or competent authorities. Then coordination centres can share this information with other emergency authorities and other critical infrastructures in case of an emergency incident.

The partners ATOS and APS of the PHOENI2X project have been involved in the development of this standard.

CEN / CENELEC CWA 18023

This CEN Workshop Agreement (CWA 18023:2023) has been developed in accordance with the CEN/CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2023-07-05, the constitution of which was supported by CEN following the public call for participation made on 2022-02-15. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2023-07-24.

This document provides requirements and recommendations for a common set of information, datatypes and terms to be reported and provided by affected critical infrastructures to national or local coordination centres or control rooms of emergency services or competent authorities. Then coordination centres can share this information with other emergency authorities and other critical infrastructures in case of an emergency incident.

The standard has reached the CWA stage. Further activities regarding the future of this standard have not been released yet.

The partners ATOS and APS of the PHOENI2X project have been involved in the development of this standard.

4.3.4 ISO/IEC JTC 1/SC 27/WG1

The subject of WG1 of ISO/IEC JTC 1/SC 27 covers standards related to Information Security Management Systems.

APS, a partner of the PHOENI2X project, is a member of this working group and works on providing feedback on the relevant requests and assignments. Standards published within this year include also ISO/IEC 27035-1:2023 and ISO/IEC 27035-2:2023 related to incident response.

4.3.5 OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC, with the CACAO Security Playbooks Version 2.0 standards

To defend against threat actors and their tactics, techniques, and procedures organizations need to detect, investigate, prevent, mitigate, and remediate threats in cyber relevant time. To do this, organizations need to identify, create, document, and test the orchestration steps needed to achieve these outcomes. These steps, when grouped together, form a cyber security playbook that can be used to protect organizational systems, networks, data, and users. This specification defines the schema and taxonomy for Collaborative Automated Course of Action Operations (CACAO) for cyber

security playbooks and describes how these playbooks can be created and shared in a structured and standardized way across organizational boundaries and technological solutions.

UiO is one of the main contributors of the CACAO standard and leads the newest technical work "CACAO Layout Extension" that develops a mechanism to graphically represent CACAO playbooks in a consistent and interoperable manner. In addition, UiO made aavailable CACAO JSON validation schemas for the global community[88].

4.3.6 OASIS Cyber Threat Intelligence (CTI) TC, with the STIX and TAXII standards

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

UiO contributes to the development of STIX 2 for a number of years. In addition, PHOENI2X results have been open sourced and operationalized by the CTI community, particularly STIX 2.1 extensions for sharing security playbooks[89].

4.3.7 OASIS Threat Actor Context (TAC) Technical Committee, creating a knowledge framework that enables semantic interoperability of threat actor contextual information

Today, organizations that share cyber threat intelligence are confronted by multiple schemas and a plethora of nonstandardized and ambiguous vocabularies. These limit an organization's ability to strategically correlate and analyze attack data, which could lead to a better understanding of their adversary's goals, capabilities, and trends in targeting and techniques.

The TAC TC seeks to resolve ambiguity across different sources and solutions to support organizing what is known and sharing information about threat actors. The TC will establish a common knowledge framework that enables semantic interoperability of threat actor contextual information and develop standardized vocabularies for threat actor characterization.

UiO chairs the effort and has been developing the Threat Actor Context (TAC)[90] ontology, supported and operationalized by PHOENI2X.

4.3.8 OASIS Open Command and Control (OpenC2)

Cyberattacks are increasingly sophisticated, less expensive to execute, dynamic and automated. The provision of cyber defense via statically configured products operating in isolation is untenable. Standardized interfaces, protocols and data models will facilitate the integration of the functional blocks within a system and between systems. Open Command and Control (OpenC2) is a concise and extensible language to enable machine-to-machine communications for purposes of command and control of cyber defense components, subsystems and/or systems in a manner that is agnostic of the underlying products, technologies, transport mechanisms or other aspects of the implementation. It should be understood that a language such as OpenC2 is necessary but insufficient to enable coordinated cyber responses that occur within cyber relevant time. Other aspects of coordinated

[88] https://github.com/cyentific-rni/cacao-json-schemas
[89] https://github.com/cyentific-rni/stix2.1-coa-playbook-extension
[90] https://github.com/oasis-open/tac-ontology

cyber response such as sensing, analytics, and selecting appropriate courses of action are beyond the scope of OpenC2.

In the context of OpenC2 and PHOENI2X, UiO has developed the actuator profile for endpoint response (ER)[91]. In particular: This Actuator Profile defines OpenC2 Actions, Targets, Specifiers, and Command Arguments in the context of response functionalities found in EDR technologies. The Endpoint Response (ER) specification is consistent with Version 1.0 of the OpenC2 Language Specification.

4.3.9 ETSI Cyber Security Technical Committee (TC CYBER)

ETSI TC CYBER is recognized as a major trusted centre of expertise offering market-driven cybersecurity standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. It works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. TC CYBER is the most security-focused technical committee in ETSI, and we have many strands of work. This roadmap describes each of TC CYBER's key areas where standardisation can help on the journey to better security.

UPAT has been involved in ETSI's standardization activities and participated in some of its specification's groups e.g. ETSI ISG INS. Even though UPAT is currently not a member of the TC CYBER, it has participated in the past in some of its meetings to present other EU projects for cybersecurity in critical infrastructures (e.g. CIPSEC). Furthermore, UPAT is leading the ETSI Software Development Group for OpenSlice which is developing an open-source service based Operations Support System (OSS) to deliver Network Slice as a Service (NSaaS). Through these connections UPAT will investigate and identify possible connections with security related WGs inside ETSI, like TC CYBER.

[91] https://github.com/oasis-tcs/openc2-ap-er/tree/working

5 STAKEHOLDER ENGAGEMENT AND LIAISON ACTIVITIES

5.1 Objectives of Task 6.3. on stakeholder engagement and liaisons

This task focuses on the engagement of entities that could potentially adopt PHOENI2X (e.g., OES, National Authorities, private and public SOCs), as well as other EU cybersecurity stakeholders (ENISA, CSIRTs network, CERT-EU, Europol, ISACs) and policy makers who can potentially provide valuable feedback but also promote the wider adoption of the PHOENI2X approach.

5.2 Stakeholder engagement methodology and initial activities

5.2.1 Introduction

The International Organization for Standardization (ISO), defines a stakeholder as "person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity" (ISO/TS 37008:2023).

Stakeholder analysis has always been important because stakeholders can substantially contribute to the success or failure of a new business. In Paul Nutt's Why Decisions Fail (2002), a careful analysis of 400 strategic decisions, Nutt finds that half of the decisions "failed" – that is, they were not implemented, only partially implemented, or otherwise produced poor results – in large part because decision makers failed to attend to the interests of and information held by key stakeholders. Other quantitative studies report broadly similar findings with respect to the importance of paying attention to stakeholders (e.g., Bryson, Bromiley and Jung, 1990; Bryson and Bromiley, 1993). Failure to attend to the information and concerns of stakeholders is clearly a kind of flaw in thinking or action that too often and too predictably leads to poor performance, outright failure, or even disaster. Stakeholder analyses are arguably more important than ever because of the increasingly interconnected nature of the world. Choose any public problem – economic development, poor educational performance, natural resources management, crime, AIDS, global warming, terrorism – and it is clear that "the problem" encompasses or affects numerous people, groups, and organizations. No one is fully in charge; no organization "contains" the problem. Instead, many individuals, groups, and organizations are involved, or affected, or have some partial responsibility to act. Figuring out what the problem is and what solutions might work are actually part of the problem (Bryson and Crosby, 1992; Bardach, 1998).

Stakeholder management emerged in the mid-1980's in the business world from the need for "a framework that was responsive to the concerns of managers who were being buffeted by unprecedented levels of environmental turbulence and change" (Freeman and McVea, 2001, p.2). Its purpose was to "devise methods to manage the myriad groups and relationships that resulted in a strategic fashion" (Freeman and McVea, 2001, p.3) "In this shared-power world, no one is fully in charge; no organization 'contains' the problem. Instead, many individuals, groups and organizations are involved or affected or have some partial responsibility to act." (Bryson, 2004, p.23)].

In the PHOENI2X project, partners have recognized the importance of the stakeholders in the PHOENI2X ecosystem and have decided to adopt a stakeholder engagement methodology comprising the following steps:

- Step 1: Setting engagement objectives
- Step 2: Implementing stakeholder analysis
- Step 3: Development of the engagement plan
- Step 4: Implementing the engagement plan
- Step 5: Assess and report the results of the engagement plan

The main focus of the first period of the project (M1-M18) have been Steps 1 – 2 as well as the identification of and consensus on the basic principles for Step 3. Steps 4-5 will be actually performed in the second period of the project (M19-M36).

5.2.2 Step 1: Engagement objectives

As a result of the project partners' collaboration, while exchanging complementary know-how, expertise, experience and opinions during their interactions (physical and virtual meetings), the following objectives of a stakeholders' engagement strategy were defined:

- to collect information/feedback from the stakeholders formulating the PHOENI2X environment to help in the design, the development and the validation of the PHOENI2X solution and the tools,
- to achieve the maximum project visibility and further promote the final PHOENI2X solution as a whole and the different tools comprising it, through connecting with a range of stakeholders,
- to raise awareness regarding the project objectives/activities/results/products among the full range of potential stakeholders.

5.2.3 Step 2: Stakeholder analysis

As mentioned in the introduction, the identification and interaction with stakeholders is very important during the design of the project outcomes and for the exploitation of the project results.

Task 6.2 allowed the project partners to identify the possible exploitable results of the project during the project time course and at the end of the project. The results of Task 6.2, helped also in the determination of the groups of stakeholders per result.

The identified groups of stakeholders are the following:

- **Critical infrastructure organizations** (CIOs) (e.g. in energy, transportation, health domains) or in general, organizations with obligations stemming from regulatory frameworks such as GDPR, NIS, eIDAS.
- **Other organizations** (SMEs/MEs, business entities, companies, organisations from any sector) interested in gaining knowledge or acquiring tools related to incident response, business continuity and incident response playbooks and in general, in making the incident response process more effective.
- **Security service providers/experts** and other **EU funded R&D projects**' participants focusing on the implementation of security measures and the implementation of effective and automated incident response procedures.
- **Policy makers** at any level (Ministries and Governments, Regulatory Agencies, other related European and national agencies, Standard Developing Organizations, etc.).
- **Greater public** (not specific)
- **Partners** of the PHOENI2X project
- **Technology organizations** (competitors)

Each one of these groups of stakeholders has different characteristics in terms of interest for the project results, influence and power over the project outcomes, which have been analyzed and assessed by the PHOENI2X partners. The assessment was benefited from the partners' complementarity within the project Consortium and the fact that the project partners represent the

above groups quite sufficiently, in terms of their business activities, while having a holistic assessment perspective depending on the different and sometimes overlapping roles they may have.

The assessment of the stakeholders was reflected in a ranking process through which the partners determined the level of interest each stakeholder has in the project and the degree of influence and power they may have over its outcomes. The ultimate goal of this assessment was to prioritize the stakeholders to be involved and then decide on the appropriate engagement strategy for each one of them. The ranking was based on the following Guidelines and scales:

Interest Scale

Low Interest (1-2): Stakeholders who have minimal concern or stake in the project or decision;

Moderate Interest (3): Individuals or groups with a reasonable level of concern or interest in the project. They have some stake in the outcome but may not be highly engaged;

High Interest (4-5): Stakeholders who are deeply concerned, engaged, or invested in the project's success or outcome. The outcome significantly affects them.

Influence Scale

Low Influence (1-2): Stakeholders whose opinions or actions have little effect on the project's outcome;

Moderate Influence (3): Those who can sway the decision or project to some extent but not overwhelmingly;

High Influence (4-5): Individuals or groups whose opinions or actions can substantially impact the project's outcome.

Power Scale

Low Power (1-2): Individuals or groups with minimal control, authority, or resources related to the project or the project results;

Moderate Power (3): Those who have some control or influence but not the highest level;

High Power (4-5): Stakeholders with significant control, authority, or resources that can greatly affect decisions at a national, regional or European level on the related subjects.

Partners ranked the stakeholder groups and the overall result is depicted in Table 15:

Table 15 Ranking of Stakeholders' groups in terms of interest, Influence and Power

Stakeholder Group	Interest	Influence	Power
Critical Infrastructure Organizations (CIOs)	**4,6**	3,7	3,1
Other organizations	3,3	2,2	1,5
Security service providers/experts & EU-funded R&D projects	**4,1**	3	2,4
Policy makers	**4,3**	**4,4**	**4,6**
Greater public	2,4	1,3	1,6
Partners of the PHOENI2X project	**4,8**	**4,4**	3,3
Technology organizations (competitors)	3,8	2,2	1,7

The stakeholders that got the highest scores (> 4) are depicted in Table 15 highlighted in red. The results are completely justified.

The CIOs, responsible for sectors such as energy, transportation, healthcare, finance, water, and telecommunications, play a crucial role in the functioning of societies and understand that

cybersecurity is not only a technical issue, but a strategic imperative for the sustainability and reliability of critical infrastructure services. The interest of CIOs in the development and implementation of effective Cyber Resilience Frameworks is related to a number of reasons, such as:

- CIOs' Dependency on Information Technology (IT) for their operations. Any disruption or compromise of their IT systems can have severe consequences on the functionality and reliability of these critical services. For example, electric utility companies in the energy sector heavily rely on IT for power generation, transmission, and distribution. Indicatively, the 2015 cyber-attack on Ukraine's power grid highlighted the vulnerability of energy infrastructure to cyber threats[92].
- Economic Impact: Disruptions to CIOs' services can lead to financial losses not only for the organizations themselves, but also for the broader economy, affecting businesses, consumers, and government revenue. For example, banks and financial institutions, face substantial economic losses in the event of a cyber-attack, impacting not only the institutions but the broader economy[93].
- National Security Concerns: An attack on critical infrastructure can have cascading effects on a nation's ability to respond to emergencies, maintain public order, and protect against external threats. For example, national government agencies, overseeing defense and emergency response functions, understand that cyber-attacks on government systems can compromise national security[94].
- Protection of Sensitive Data: Critical infrastructure often involves the processing and storage of sensitive and personal data. CIOs are responsible for safeguarding this information to ensure the privacy and trust of the individuals and entities involved. A resilient cybersecurity framework is essential to prevent unauthorized access and protect sensitive data from theft or manipulation. For example, hospitals and healthcare providers, integral to the healthcare sector, prioritize cyber resilience to protect sensitive patient data and ensure uninterrupted healthcare services[95].
- Maintaining Public Trust: The public relies on critical infrastructure services for their daily lives. Any disruption or compromise in these services erodes public trust. An effective Cyber Resilience Framework is crucial for preventing and mitigating cyber incidents, thereby preserving the trust of the communities they serve. For example, railways, airports and air traffic control systems, essential to the transportation sector, rely heavily on interconnected systems and recognize the importance of public trust and safety, which can be compromised in the event of a cyber-incident affecting smooth operations, flight schedules, etc.[96, 97]
- Regulatory Compliance: The importance of cybersecurity in critical infrastructure is increasingly being recognized by Governments and regulatory bodies. Many countries (see EU has (NIS) Directive and (GDPR), Germany has IT Security Act (BSI-Gesetz), UK with NCSC, USA with CISA and (NIST), etc.) have enacted or are in the process of developing regulations that

[92] https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine
[93] https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/
[94] https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks
[95] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health
[96] https://www.railway-cybersecurity.com/Railway_cybersecurity.html
[97] https://www.icao.int/aviationcybersecurity/Pages/default.aspx

mandate certain cybersecurity standards for CIOs and the latter have a vested interest in complying with these regulations to avoid legal consequences and reputational damage. For example, water treatment plants in the water and wastewater sector comply with regulations (e.g. EU NIS Directive, EPA guidance) to protect water infrastructure and public health from the consequences of a cyber-attack on water systems.

- Continuous Threat Evolution: CIOs recognize that a static security posture is insufficient to protect against the ever-changing tactics of cyber adversaries. An effective Cyber Resilience Framework provides the agility and adaptability needed to respond to new and emerging cyber threats. For example, telecommunication service providers understand the need for an agile and adaptable Cyber Resilience Framework to ensure the continuous and secure operation of communication networks[98].
- Business Continuity: A resilient cybersecurity framework helps organizations recover quickly from disruptions, minimizing downtime and ensuring that critical services remain operational even in the face of a cyber incident. For example, the government sector, especially national government agencies, recognizes the importance of maintaining business continuity in essential services such as defense, intelligence, and emergency response[99].

From another perspective, Security Service Providers and Researchers have a significant interest in the development and implementation of effective Cyber Resilience Frameworks for several compelling reasons, such as to:

- Enhance Industry Reputation and Credibility: An effective Cyber Resilience Framework is crucial to demonstrate commitment to providing reliable and robust cybersecurity solutions while aligning with established frameworks.
- Stay Ahead of Evolving Threat Landscape: A Cyber Resilience Framework provides a structured approach to understanding and mitigating evolving cyber risks, enabling them to offer cutting-edge solutions.
- Build Client Trust and Satisfaction: A robust Cyber Resilience Framework allows service providers to demonstrate their commitment to providing comprehensive security measures.
- Ensure Efficient Incident Response and Recovery, including established processes and procedures, minimizing downtime and reducing the impact of security breaches.
- Promote Research and Innovation: A Cyber Resilience Framework provides a foundation for conducting research on emerging threats and vulnerabilities, leading to the development of novel security solutions and strategies.
- Ensure Regulatory Compliance, including relevant laws and standards pertaining to cybersecurity to avoid legal consequences.
- Enforce Continuous Improvement and Adaptability, by staying proactive in updating their strategies and solutions.

[98] https://pf.content.nokia.com/t007es-trust-netguard-cybersecurity-dome/article-cybersecurity-for-csp?did=D00000005659&utm_campaign=CYSD_demand_2023&utm_source=nurture&utm_medium=email&utm_content=&utm_term=&mkt_tok=OTM3LVdSWi02MTgAAAGPvtx5J_C5HMT4_fCdSMHSNvZMTgfsBv189IzDeCZ-UhFY-Sw_PMxkRcXPnTcjJLTTySr-sZ3VwOjdUkeoQiCPww29swFhUqw9h3S71jj0t8Szdw&xs=472506

[99] https://www.sentinelone.com/blog/why-governments-and-agencies-are-targeted-by-cyber-attacks-a-deep-dive-into-the-motives/

- Facilitate Information Sharing and Collaboration, considering that cyber threats are often transnational and can affect multiple organizations, which indicates a collective approach to addressing common cyber threats and vulnerabilities.
- Gain Market Competitiveness, in the highly competitive cybersecurity market especially when clients are evaluating different providers for their security needs.

As far as the PHOENI2X partners' interest is concerned, this is undoubtedly high, provided that in the context of the project they are given the opportunity to collaborate with experts of the industry and the research community and join forces while being funded. Under such privileged conditions, they can pursue innovation and gain competitive advantage through outcomes significantly differentiated in the market . As already mentioned, practically all the stakeholders' groups are represented in the Consortium. Indicatively, PPC, FGC, NPS and COSM are representatives of the CIOs ecosystem, obviously having their "competitive" cyber-security framework already in place and sometimes being themselves security solution providers (e.g. COSM); NCSA and DSA are State authorities entrusted with cybersecurity with primary involvement in the validation of the cyber-resilience processes and EUNL with primary role in ethical and IPR issues, thus playing "a policy makers" role. On the other hand, SANL, AEGIS, ATOS, APS, WS, SEA are business/legal entities (of different size and focus from the CIOs) interested in enhancing existing technological offerings and increase their business capacity. In addition, the Academic and Research Institute partners (UOP, UPC, UiO), are also interested in enriching their technological expertise in the area of cyber-security measures and the implementation of effective and automated incident response procedures. Obviously, as partners of the PHOENI2X consortium and with vast experience in R&D projects, all are working on the common goal of the project success. Above all, they are the ones to have a major influence on the project outcomes participating in all the critical stages of design, development, testing and validation, provided that they are committed to take advantage of all the available human and technical resources throughout the project duration.

Among the groups of the PHOENI2X stakeholders, the group that scored the highest in all the 3 categories (interest, influence, power) has been that of the policy makers. For reasons that have been already mentioned (see the CIOs' interest), the policy makers have a substantial interest, too, in an effective PHOENI2X-like Cyber Resilience Framework for CIOs, due to national security, public safety and economic considerations. More specifically, such a Framework for CIOs helps prevent and mitigate cyber threats, protect sensitive information crucial to national interests, maintain the integrity of government operations, ensure public safety and continuity of essential services. On the other hand, it can reduce the risk of cyber incidents that could impact businesses, supply chains, and overall economic infrastructure; thus, contributing to economic stability.

In addition, policy makers possess the authority to strongly influence the Cyber Resilience Framework for CIOs through legislation and regulation. They can enact specific laws and regulations which define the requirements for the Framework development and implementation, establishing legal standards that CIOs must adhere to. In addition, policy makers can mandate compliance requirements with cyber security standards for CIOs; thus, guiding them in aligning with national cyber security objectives. Besides, the policy makers can financially support initiatives aimed at enhancing the cyber security resilience of CI; thus, incentivizing CIOs to invest in robust Cyber Resilience Frameworks.

Moreover, policy makers have the power to drive changes in these Frameworks adopted by CIOs at national, regional, or European levels. Firstly, they can establish enforcement mechanisms and penalties for non-compliance with cyber security regulations. This power motivates CIOs to prioritize and implement changes in their Cyber Resilience Frameworks to avoid legal consequences. Furthermore, policy makers play a central role in shaping national cybersecurity strategies that include

directives and guidelines for CI resilience, as well as in the development of global and regional agreements and standards for international collaboration of CIOs on cybersecurity issues. Policy makers can establish and promote information-sharing platforms (regarding intelligence and best practices) that facilitate collaboration among CIOs and contribute to the evolution of effective Cyber Resilience Frameworks.

The above analysis has led to two (2) greater groups of Stakeholders, one of higher and another of lower priority, as depicted in Table 16:

Table 16 Prioritization of Stakeholders' Groups

Order	Stakeholder Group – Priority 1	Stakeholder Group – Priority 2
1	Policy makers	Technology organizations (competitors)
2	Partners of the PHOENI2X project	Other organizations
3	Critical Infrastructure Organizations (CIOs)	Greater public
4	Security service providers/experts & EU-funded R&D projects	

5.2.4 Step 3: Development of the engagement plan

Based on the result of the Step 2, the focus of the engagement activities shall be put on the group of Priority 1 with very specific and demanding engagement strategies on a per stakeholder basis to gain further insights on the needs and expectations of stakeholders. Besides, engagement plans for the group of Priority 2 will be implemented, mainly in the context of the dissemination activities.

In both cases, the strategies will take advantage of various communication channels or methods for engaging with each stakeholder. This can include face-to-face (f2f) meetings, expert interviews, surveys/questionnaires (either standalone or as part of a workshop), emails, phone calls, social media, or specific platforms.

As far as the surveys/questionnaires are concerned, four (4) main pillars will be investigated:

- The current cybersecurity solution in place at the entity.
- The gaps identified and further needs considered by the entity.
- Recommendations on gaps and needs by the PHOENI2X partners.
- Evaluation of the PHOENI2X solution capability of addressing additional/emerging needs.

The main characteristics of the engagement strategies per stakeholder are provided in Table 17 and Table 18:

Table 17 Engagement strategy for Stakeholder Group – Priority 1

Stakeholder Group – Priority 1	Engagement Plan	Leading partners	Plan
Policy makers	At least 3 activities focusing on regulation and standards	NCSA, DSA, EUNL, APS, UiO	1 per semester (S4, S5, S6)
Partners of the PHOENI2X project	At least 5 expert interviews	COSM,	1-2 per semester (S4, S5, S6)
Critical Infrastructure Organizations (CIOs)	Exploring the needs and feedback of at least 3 (external to the project) CIOs through targeted surveys	FGC, PPC, WSE, APS, NPS	1 per semester (S4, S5, S6)
Security service providers/experts & EU-funded R&D projects	- Exploring the needs and feedback of 3 security service providers through targeted surveys - Liaison activities with R&D projects (Keep an ongoing	COSM ALL	1 per semester (S4, S5, S6)

	cooperation between R&D projects, Participation in at least 3 joint activities)		

Table 18 Engagement strategy for Stakeholder Group – Priority 2

Stakeholder Group – Priority 2	Engagement Plan	Responsibilities	Plan
Technology organizations (competitors)	- Invitations in at least 3 conferences/workshops - Participation in events with other stakeholders - Posts on the social media	At project level	During the whole P2
Other organizations	- Invitations in at least 3 conferences/workshops - Participation in events with other stakeholders - Posts on the social media	At project level	During the whole P2
Greater public	Dissemination activities (posts on the social media, project Newsletters, videos, etc.)	At project level	During the whole P2

An indicative list of engagement activities planned for P2 (M19-M36) is provided in Table 19:

Table 19 Engagement activities planned for P2 (M19-M36)

#	Stakeholder	When (MM/YYYY)	Where (Physical location, online)	Focus of activity (PHOENI2X as a whole, specific component)	Activity (presentation, workshop, email, survey, talk, etc.)	Expected Outcome (1-2 phrases)	Responsible partner
1	CIOs & Energy stakeholders	Oct-24	Enlit Europe 2024, Milan, Italy	Engagement with relevant energy stakeholders	f2f discussions, possible presentation of PHOENI2X	Evolution in cybersecurity in the energy domain	PPC
2	CIOs	Jan-24	Online	PHOENI2X as a whole	email, possible presentation of PHOENI2X, banner	Promote the PHOENI2X solution and gain insights from relevant organizations about their interest in adopting the solution	DSA
3	Representatives from similar cybersecurity projects	Mar-24	FIC Forum, Lille, France	PHOENI2X as a whole	f2f discussions, possible presentation of PHOENI2X	Synergies and collaboration with similar cybersecurity projects	AEGIS
4	CIOs	2024 2025	Online	PHOENI2X as a whole	Press Release/ Leaflet	Gain a broad reach over the whole ecosystem of entities and relevant	NCSA

						organisations and promote the project.	
5	PHOENI2X Project Partners	2024 2025	Online	NIS2-initiated obligations and relevant guidelines that affect PHOENI2X. Focus on: - Incident Reporting and Handling - Compliance challenges	Presentation/ Workshop	Discuss/ Highlight project contribution in: • Compliying with the new regulatory obligations • Implementing the updated Incident Response and Reporting processes. • Supporting entities and authorities during the transposition period.	NCSA
6	ELECTRON project	Jan-24	Telco / physical meeting	datasets for training AI algorithms	Discussion	Discussion about datasets that ELECTRON project provides and PHOENI2X can benefit of and other topics of collaboration	UPAT
	Hellenic Trains	2024	Telco / physical meeting	PHOENI2X project	Presentation of PHOENI2X	Identify possible contributions and future collaborations	UPAT
7	CIOs	Dec-24	DSA Annual Stakeholder meeting, Nicosia, Cyprus	Engagement with OES	Presentation and bilateral discussions	Exploring of needs, feedback on the solution	DSA
8	Policy Makers	Mar-24	2nd ENISA Cybersecurity Policy Conference	PHOENI2X as a whole	bilateral discussions	Identification of trends, needs and development in cybersecurity policy	TBD
9	Policy Makers	Mar-24	EU Cyber Acts 2024	Security Automation and Orchestration /	Presentation and bilateral discussions	Awareness of contributions to	UiO

				Standardization efforts through Phoeni2x		standardization (CACAO) and PHOENI2X activities regarding implementation	
10	Security service providers/experts & CIOs	Jun-24	FIRSTCON	Phoeni2x component (ROAR)	Presentation and bilateral discussion	Awareness of contributions to standardization (CACAO) and PHOENI2X activities regarding implementation	UiO

5.2.5 Step 4: Implementing the engagement plan

Although the stakeholders will be engaged in the next project period until the end of it, some initial activities have already been performed, such as those listed in Table 20:

Table 20 Engagement activities performed in P1 (M1-M18)

#	Stakeholder	Date	Location	Focus of activity	Activity	Conclusions	Responsible partner
1	DSOs, manufacturers of smart meters, technology providers in the energy sector.	Nov-23	Enlit Europe 2023, Paris, France	current state of cybersecurity & requirements on AMI	f2f discussions	In some cases, the smart meters can be connected online through the residential Internet access. This validates our assumption in UC1 about exposure to threats and the larger attack surface that this setup entails.	PPC
2	Representatives from similar cybersecurity projects	Apr-23	FIC Forum, Lille, France	PHOENI2X as a whole	f2f discussions	Creating opportunities for synergies and collaboration	AEGIS
3	Suppliers and consumers of cybersecurit	Sep-23	ENISA Cybersecurity Market Analysis event,	PHOENI2X as a whole, FVT as a product/service	f2f discussions with stakeholders	Deepening in current state of cybersecurity market forces and their	AEGIS

	y services, regulators of cybersecurity products, services or processes, research organisations, market analysts		Crete, Greece			interplay, as well as in the emerging threat landscape and industry response in terms of product and service development	
4	ELECTRON project	Dec-23	Telco	datasets for training AI algorithms	discussion	Discussion about datasets that ELECTRON project provides and PHOENI2X can benefit of. A new telco (beg/2024) agreed to organize a joint physical meeting or activity.	UPAT
5	ECSO	Nov-23	Online	NIS2 Implementation Initiative: Public Authorities of Luxembourg and Czechia	workshop and task force participation	There will be a joint white paper related to NIS2 issues	ATOS
6	EU-CIP	Nov-23	Online	Advisory board meeting of CIP projects	Chairman of AB	Collaboration, knowledge sharing and roadmapping in the area of critical infrastructure protection in EU	ATOS
7	ECSCI	May-23	Online	Collaborative Standardisation and Policy Making For Greater CI Resilience in Europe	workshop (remote participation)		ATOS
8	COMSA	June 2023	UITP Summit, Barcelona	Phoeni2x as a hole and importance of Cybersecurity in the future of Railway	Discussion	Collaboration, knowledge sharing, and possible interest in	FGC

						evolution of the project	

5.2.6 Step 5: Assess and report the results of the engagement plan

For every engagement activity to be performed an assessment process will be performed. The process depends on the type of results derived. Indicatively, in face-to-face meetings, the minutes of meeting will be analyzed and related with the project activities and goals and the highlights will be reported. After an expert interview, again the relation with the project will be identified along with potential highlights will be reported. The results of each survey will be assessed by the consortium to identify how the project can be benefitted. In addition, the results of all the surveys will be assessed comparatively, if applicable. Last but not least the dissemination KPIs will be monitored on a continuous basis.

5.3 Liaison activities

5.3.1 Liaison with R&D projects

Especially for the R&D projects (sub-category), the PHOENI2X partners pursue opportunities for joint activities to exchange knowledge/expertise on issues of common interest, like those listed in Table 21:

Table 21 Joint events of PHOENI2X with other R&D projects

Partner	Event	Date	Location	Type of action
UPAT COSM	Infocom 2023 Workshop "Modern R&D Projects: Creating the Pillar for Investment and Innovations in the ICT Converged (Vertical) Markets"	12/14/2023	Athens	Presentation of PHOENI2X at a workshop with 25 other EU-funded projects, incl. CyberSecDome and RE-WIRE projects
UPC	DRCN 2023 Panel: "Reliability, are you for real?" with the DRCN2023 conference	18/04/2023	Vilanova	Presentation of PHOENI2X at an Industrial Panel
UPC	4th International workshop on Information & Operational Technology (IT & OT) security (IOSEC 2023) in conjunction with the DRCN2023 conference	20/04/2023	Vilanova	Organization of a workshop jointly with 3 EU-funded projects (JCOP, IntellIoT, and FISHY)
AEGIS	4th International workshop on Information & Operational Technology (IT & OT) security (IOSEC 2023) in conjunction with the DRCN2023 conference	20/04/2023	Vilanova	Attended the workshop. Promoted PHOENI2X in networking discussions.
UPAT	CYBERHOT summer school	29-30/03/22 29/09/2023	Crete	Sponsoring and Participating in "Cybersecurity Hands -On - Training (CyberHOT)" that takes place every year in Crete under the auspice of NATO
UiO	5th Annual Workshop on Cyber Threat Intelligence and Hunting	19/12/2022	Osaka	Organization of a jointly workshop with 1 other EU project (JCOP)
UiO	6th Annual Workshop on Cyber Threat Intelligence and Hunting	17/12/2023	Sorrento	Organization of a jointly workshop with 1 other EU project (JCOP)

FGC	ISBeRG (International Suburban Rail Benchmarking Consortium) Railways Biannual Meeting	10/11/2023	Barcelona	Presentation of the Innovation in FGC to ISBeRG members, and presentation of PHOENI2X Project to Railway enterprises. Also networking discussions.

In addition, the PHOENI2X partners have an active collaboration with a number of projects with similar/relevant goals, objectives, activities, expected outcomes, use cases, approaches, etc. with PHOENI2X (Table 22), whose outcomes may directly or indirectly have some impact on PHOENI2X. For the projects listed here there is one or more PHOENI2X partners involved, thus we can use their presence in the other consortium to keep an ongoing cooperation between projects.

Table 22 Engagement opportunities through R&D projects in parallel with PHOENI2X

PHOENI2X partner	ELECTRON H2020	AI4CYBER HE	DYNABIC HE	SUNRISE	CYCLOMED	FISHY	HORSE	SYNAPSE	JCOP	SENTINEL	SAND5G	CONSOLE	AInception
UPAT											x	x	
SANL								x	x	x			
UPC						x	x						
PPC	x	x	x										
AEGIS								x		x			
EUNL								x					
ATOS	x			x	x		x						
NPS								x					
UiO								x	x				x
NCSA									x				
DSA								x	x				

The relation among PHOENI2X and other R&D projects is indicated briefly through the activities of the partners.

ELECTRON (https://electron-project.eu/)

The partners PPC and ATOS participate in the ELECTRON project which aims to address the need to shield the Electrical Power Energy Systems (EPES) infrastructure against a variety of threats – from cybersecurity incidents and privacy violations to electricity disturbances and severe human errors caused by a lack of relevant training. Specifically, the project will develop a new-generation EPES platform capable of empowering the resilience of energy systems through risk assessment, anomaly detection/prevention, failure mitigation and energy restoration. PPC provides its EV charging infrastructure in order to validate ELECTRON against the detection and mitigation of relevant

cyberattacks. Moreover, PPC participates in publications and to the publication of an intrusion detection dataset about the Open Charge Point Protocol. Finally, PPC also contributes to the development of the mitigation technologies that are based on SDN and OpenFlow. ATOS is a technology provider in the ELECTRON project. It leads the WP on a Next Generation Electrical Power and Energy Systems (EPES) Cyber-defence & Protection. As a WP leader, ATOS plays an important role in the coordination and delivery of the ELECTRON's CYPER Framework, the outcome of the WP activities. Particularly, ATOS delivers an enhanced version of its XL-SIEM, called E-SIEM, for an extended situational awareness of attacks and malicious activities across different layers of an EPES infrastructure; An enhanced version of its LADS system for cybersecurity monitoring and anomaly detection in Power Grid substations covering a number of SCADA protocols such as IEC-104, DNP3, Modbus, and IEC-61850; and An ELECTRON's SharePoint solution where various EPES and other Critical Infrastructure stakeholders anonymously share with each other vulnerabilities and cybersecurity incidents.

AI4CYBER (https://ai4cyber.eu)

PPC participates in the AI4CYBER project which aims at delivering socio-technical methods, models and tools for resilience management. It will produce and validate a framework that enables system operators to forecast, assess and mitigate in real time business continuity risks and their possible cascading effects. PPC provides an energy infrastructure testbed in order to validate AI4CYBER against various advanced threats and AI-powered attacks.

DYNABIC (https://dynabic.eu/)

PPC participates in the DYNABIC project which aims at providing an Ecosystem Framework of next-generation trustworthy cybersecurity services that leverage AI and Big Data technologies to support system developers and operators in effectively managing AI-powered cyberattacks. PPC provides a case study of an EV charging infrastructure, that is used for the development of DYNABIC, a solution that aims to ensure business continuity and resilience against advanced cyber-physical threats.

SUNRISE (https://sunrise-europe.eu/)

The EU-funded SUNRISE project aims to ensure greater availability, reliability, and continuity of critical infrastructures in Europe including transport, energy, water, and healthcare. ATOS plays the role of a project coordinator and a technology provider for the SUNRISE project. ATOS plays an important role not only in project coordination but also in leadership of a WP on delivering a tool for CI's cyber-physical resilience. Particularly, ATOS provides a toolset for threat intelligence and incident response & reporting, and dynamic cyber-physical risk assessment of CIs assets in conditions of pandemics. Furthermore, ATOS is a key contributor to the work package of remote infrastructure inspection by provisioning of a visual anomaly detection & 3D model generation, and inspection of critical infrastructure using UAVs. ATOS also participates in local and national collaborations of CIs, in requirements and design of SUNRISE tools, as well as in communication and business plan definition activities.

CYLCOMED (https://www.cylcomed.eu/)

CYLCOMED aims at strengthening the cybersecurity of connected, in vitro diagnostic and software as medical devices, maintaining their performance and safety for patients and preserving or enhancing the confidentiality, integrity and availability of private data they exchange or allow to be remotely accessed and focusing on humans operating the technology as the weakest link in the chain for security and privacy, with training and awareness measures tailored to healthcare staff needs. ATOS is a technology provider in the CYLCOMED project. ATOS plays an important role leading the WP on Cybersecurity Toolbox design and implementation. Within this WP, ATOS has three major

contributions focused on the applicability of AI for the behavioural analysis of medical devices (covering network traffic analysis with unsupervised Deep Learning capable of detecting a wide range of cybersecurity incidents), the identity & access management and data protection for connected medical devices, and the CYLCOMED security dashboard integrating and processing all the security events provided by the toolbox components and providing the situational awareness picture and risk exposure of the organisation.

FISHY (https://fishy-project.eu/)

The partner UPC participates in the FISHY project which aims at developing a cyber resilient platform to enable trusted supply chains of ICT systems through AI-based security technologies and innovative methodologies for risk assessment. In FISHY UPC develops an AI-based threat detector engine, which uses ML algorithms for the detection of zero-day cyberattacks and the classification of known cyberattacks. UPC also has developed a technology for the definition of the mitigation strategies to be applied for the detected attacks.

HORSE (https://www.horse-6g.eu/)

The partners UPC and ATOS participate in the HORSE project which aims to design, develop and validate a 6G architecture providing a human-centric approach to security workflows by enabling end-to-end security solutions. In HORSE, UPC develops a technology for modelling attacks and threats, as well as their impact on the different 6G components. The generated models will be used by the Digital Tween to pre-assess security provisioning in order to proactively act to any deviation or potential issue that may come up affecting the services delivery and the overall connectivity. ATOS plays the role of technical coordinator and technology provider for the HORSE project. ATOS plays an important role in leadership of a work package on delivering an AI-assisted human-centric Secure and Trustable Orchestration. Particularly, ATOS will contribute to the design and development of mechanisms to protect the HORSE infrastructure against cyberattacks and will be a key contributor in the design and implementation of orchestrators connectors to provide a unified cross-domain resource management and orchestration stratum to the upper layers of the HORSE architecture

SYNAPSE (website N/A yet)

EUNL, AEGIS, UiO, NPS and DSA participate in the SYNAPSE project which aims at designing, developing & delivering an Integrated Cyber Security Risk & Resilience Management Platform, with holistic AI-enhanced Situational Awareness, Incident Response & Preparedness capabilities. In the context of Synapse, EUNL's main role is to ensure and monitor conformity to the privacy & ethics requirements of the project, including GDPR compliance. EUNL's contributions include in-depth analysis of the related normative frameworks and the advancement and implementation of evidence-based compliance monitoring tools. AEGIS is leading the effort to extract user/technical requirements towards creating the platform architecture. Additionally, it is responsible for establishing the baseline tools. Furthermore, it is responsible for the Information Exchange, Alerting & Reporting module. It is also a key contributor to the impact and outreach activities of the consortium. DSA's main role is overseeing of regulatory and technical aspects of healthcare pilot. Key contributor to regulatory requirements, impact, standardisation and outreach activities. Finally, UiO supports tasks on Cyber Threat Intelligence Discovery & Analytics, Cybersecurity Orchestration, Automation & Response, and the activities pertaining to Stakeholders' Engagement and EC Initiatives' Liaisons. NPS is one of the use case providers of SYNAPSE.

SENTINEL (https://sentinel-project.eu/)

AEGIS participates in the SENTINEL project which aims at bridging the security and personal data protection gap for European SMEs/MEs, by integrating tried-and-tested security and privacy technologies into a unified digital architecture and then applying disruptive Intelligence for Compliance. In SENTINEL, AEGIS is the leader of the UI-related task of the project towards creating the front-end of the platform, integrating input from all other components. Additionally, it is responsible for the market analysis and business planning efforts. It is also a key contributor to the impact and outreach activities of the consortium.

JCOP (https://jcop.eu/)

SANL, DSA, UiO and NCSA participate in the JCOP project. SANL is the technical coordinator of the JCOP project which focuses on designing, developing, and delivering a Joint Cybersecurity Operations Platform tailored to the needs of EU member state authorities entrusted with cybersecurity and according to the guidelines provided in the EU Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises. The JCOP platform is used to create a SOC cluster between DSA (in Cyprus) & NCSA (in Greece). Thus, in JCOP, DSA and NCSA are involved in the deployment of JCOP instances and usage of the platform as a national entity. Also participates in the demonstration and validation activities. NCSA is participating in JCOP, providing guidance on the regulatory framework, and insight on national and European established procedures regarding reporting and alerting. NCSA also contributes in validating the project products and acts as an end user. UiO supports the delivery of components regarding the exchange of security playbooks, alerting and reporting of cyber incidents at machine speed, and relevant standardization activities.

AInception (https://www.ainception.eu/)

UiO participates in AInception which aims to develop novel AI-based tools and techniques for detection and response: from detecting adversarial behaviour from logs and network traffic; to understanding, contextualizing and explaining the detected threat; to generating risk and impact aware response action; all the way to automating the execution and evaluation of the response action on the underlying infrastructure. AI will play a central role for all these steps in the AInception tool pipeline. These tools will be combined into a proof-of-concept end to-end detection and response prototype, evaluated in operational scenarios with end users. UiO supports the project in the context of creating knowledge graphs and reasoning capabilities in the context of cyber threat intelligence and develops OpenC2 actuator profiles relevant to defense sector.

5.3.2 Liaison with EU

Last but not least, the liaison activities of the project with EC initiatives, working groups (WGs), white papers (jointly with other projects), etc. are listed below. The partners take advantage of their presence and contribution already established by their organisations to represent PHOENI2X; thus, achieving the maximum project visibility and raising awareness regarding PHOENI2X and the areas touched by the project (e.g. related with Cybersecurity, AI/ML, business continuity, recovery methodologies).

Table 23 Liaison activities by ATOS

Association	**ECSO**
Work Group:	NIS2 workstream
Representative(s) on behalf of PHOENI2X	ATOS (Aljosa Pasic)
Activities and Achievements:	Preparation of contribution to the NIS2 Implementation White Paper. The White Paper will tackle main challenges & priorities in the implementation with a focus on 4 pillars:

	- NIS2 Implementation « starter pack » - Use cases of implementing organisations - Overview of transposition in the EU Member States - Survey capturing the main pain points in the implementation
Future Plans:	Partner ATOS will continue to participate actively in the workstream activities, and will channel its work to the PHOENI2X related activities. In the opposite way, work performed in the context of PHOENI2X will be used to bring value to ECSO activities.

Table 24 Liaison activities by UPAT

Association	**ETSI**
Work Group:	ETSI Software Development Group for OpenSlice
Representative(s) on behalf of PHOENI2X	UPAT (Christos Tranoris, Spyros Denazis, Kostis Trantzas)
Activities and Achievements:	- This working group is led by UPAT and is developing an open-source service-based Operations Support System (OSS) to deliver Network Slice as a Service (NSaaS). - It might not be directly linked with the security activities of PHOENI2X but the participants will investigate and identify possible connections with other WGs more relevant to security e.g. TC CYBER
Future Plans:	Investigate possible connections with WGs relevant to security e.g. TC CYBER.

Table 25 Liaison activities by UiO

Association	**ENISA**
Work Group:	AHWGs on SOC and Cyber Threat Landscapes
Representative(s) on behalf of PHOENI2X	UiO (Vasileios Mavroeidis)
Activities and Achievements:	- These working groups support the EU and ENISA identifying best practices on representing and exchanging security playbooks and creating annual, thematic, and sectorial threat lanscapes. - Know-how and results from Phoeni2x is communicated in working sessions in support of the activities of the working groups.
Future Plans:	UiO will continue participating in the working groups, providing expertise and communicating results pertaining to Phoeni2x.

6 CLOSING REMARKS AND FUTURE STEPS

This document provides an overview of the strategies, plans designed and activities carried out by the PHOENI2X project partners, as part of Tasks 6.1. (Communication & Dissemination Activities), 6.2 (Impact creation, Exploitation & Standardisation activities) and 6.3 (Stakeholder Engagement and EC Initiatives' Liaisons).

Project partners are steadily involved and results are produced under the leadership of each task leader.

In relation to Communication & Dissemination, the project visual identify has been created, the website and social media of the project have been activated and content is added, newsletters have been created and circulated and the project partners have organized and participated in a number of events. It should be noted that several publications have been issued by the project partners and a relevant brochure and poster created and affixed on the website to be used as needed.

In relation to Impact creation, Exploitation & Standardisation activities, surveys and discussions have taken place to gather information on the exploitation potential of the project solution and its components. The surveys resulted in the identification of 21 exploitable results which (with the feedback of the partners) were subsequently ranked and KERs were identified. For the KERs, an initial identification of the market, its size, the potential, the key player and an identification of issues regarding patentability and IPR were researched and documented. An approach for the valorization of the project results through standardization has been defined and has already yielded results.

In relation to Stakeholder Engagement and EC Initiatives' Liaisons, a methodology has been created regarding the identification and ranking of the stakeholders. Based on the results of the ranking, engagement approaches have been selected for each stakeholder group and an engagement plan has been created. The results of the activities of the project partners related to Stakeholder Engagement and EC Initiatives' Liaisons are also presented.

In each case, the strategy, plans and activities are identified and shall be followed during the next months of the project as described in the relevant sections. Performance will be monitored through relevant KPIs (where applicable) and discussions between the project partners. If during the implementation of the planned activities, the project partners identify any issues or concerns regarding their effectiveness arises, the plans will be modified as needed, in order to ensure effective implementation of the project and the enhancement of the project results.

7 ANNEX 1.

HORIZON EUROPE PROGRAMME
HORIZON-CL3-2021-CS-01-01

PHOENIIX

A EUROPEAN CYBER RESILIENCE FRAMEWORK WITH ARTIFICIAL INTELLIGENCE -ASSISTED ORCHESTRATION & AUTOMATION FOR BUSINESS CONTINUITY, INCIDENT RESPONSE & INFORMATION EXCHANGE

ERs Identification

Contractual Date of Delivery	
Actual Date of Delivery	
Deliverable Security Class	
Editor	*[Full name (Partner Acronym)]*
Contributors	[Partner Acronyms]
Quality Assurance	

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No 101070586

PHOENIIX GA No. 101070586

1 Introduction to Exploitable Results

According to the Horizon 2020 text, a result is defined as:

"Any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights".

Exploitable Result (ER) is considered any form of intangible project result (technical consulting, business consulting, system integration capacity), or tangible result (software component, library, tool, prototype, service suite, etc.).

A Key Exploitable Result (KER) is an identified main interesting result (as defined above) which has been selected and prioritized due to its high potential to be "exploited" – meaning to make use and derive benefits- downstream the value chain of a product, process or solution, or act as an important input to policy, further research or education.

As a first step regarding the organization of the exploitation planning, with your help we would like to identify the Exploitable Results of the PHOENIIX project. After the collection of the ERs, we will run another process to identify the KERs.

Each partner is asked to identify at least one Exploitable Results as an owner or co-owner / developer. The information on the Exploitable results should be provided per identified ER. If you have identified more than one ER, replicate the structure accordingly or create a separate document.

1.1 Basic Information

Partner / Owner	
Contact Information	
Name and description of the Exploitable Result	
Type of result (product, process, software, service, etc.)	

PHOENIIX GA No. 101070586

List of main functionalities (Top 3-5 functionalities in bullets (max 1 sentence each))	
Expected project month of first deliverable of ER (e.g., M36, etc.)	
Exploitation Path of ER: To be used in partner's own premises / internally? | To be exploited commercially? (e.g., via license, service, etc.? | To be open-sourced to the community | To be used in future research?)	

1.2 Assistance

Requiring help for promotion / dissemination / communication from the relevant task of WP6

Further help that would be needed from this task (e.g., help in PR, IP protection, business model generation, etc.)

PHOENIIX GA No: 101070586

1.3 Technical Maturity

Where a topic description refers to a TRL (Technology readiness levels), the following definitions apply, unless otherwise specified:

According to the above-mentioned definitions, please filled in the table below.

Technical maturity of the ER at the start of the project:	
Current technical maturity of the ER:	
Envisioned technical maturity of the ER at the end of the project:	

PHOENIIX GA No. 101070586

1.4 Market demand or readiness level

What is the current contribution to or positioning in the specific market (Competitors or alternative solutions)?

Which industrial sector does the ER target or is relevant with?

1.5 Value Proposition Canvas

The Value Proposition Canvas was initially developed by Dr Alexander Osterwalder as a framework to ensure that there is a fit between the product and market. It is a detailed tool for modeling the relationship between two parts of the Osterwalder's broader Business Model Canvas; customer segments and value propositions.

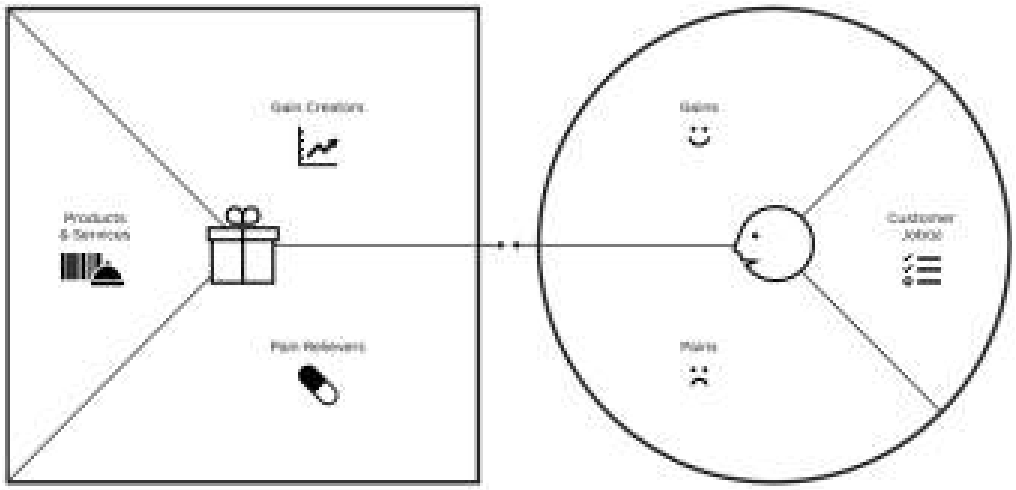
In this case we use the different components of the canvas to identify the targeted customers for the ERs of the PHOENIIX project and to learn how to fulfill their needs better through this solution.

This canvas could be providing the analysis for the main system / output of the PHOENIIX project but it could also be specific for each one of the identified ERs.

1.5.1 Step 1: Scope

Please indicate the Scope of this analysis i.e. ER Description, entire solution

PHOENIIX GA No. 101070586



1.5.2 Step 2. Fill in the information for the customer segment

1.5.2.1 Customer Jobs

Guidance:

Jobs or tasks that the targeted customer of this ER is trying to do. You have to include all tasks customers are trying to perform, the problems they are trying to solve, and the needs they want to satisfy. It's also important to note down the frequency and the importance of each job, and all the different roles the customer have to play, and in what contexts. To fulfill this step, you may ask yourself:

- *What functional tasks is my customer trying to perform? (day by day tasks, problems at work, etc.)*
- *What social tasks is my customer trying to accomplish? (get a promotion, gain status, have a network, increase reputation, etc.)*
- *What emotional tasks is my customer trying to complete? (get in shape, feel good, feel motivated, feel safe etc.).*
- *What basic needs do they need/want to have satisfied? (communication, safety, preparedness etc.).*

•

1.5.2.2 Gains

Guidance:

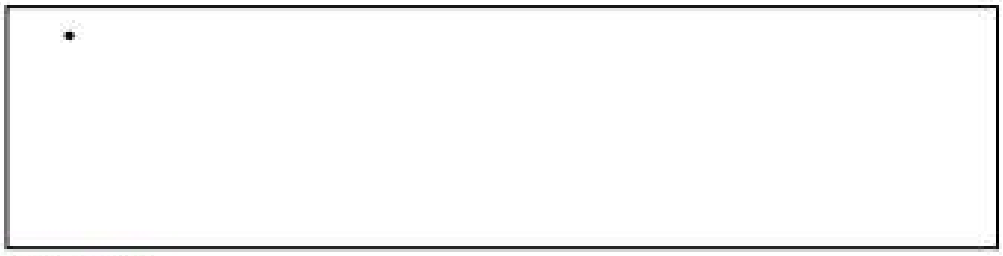
Gains are all the benefits your customer expects or wishes – or even something that would surprise them positively –, whether they are functional, emotional, social or financial. In short, everything that delight them and make their life easier, more joyful or more successful. You may rank each gain by relevance and indicate the frequency of them. To do so, you can follow some questions, such as:

- What kinds of savings would make my customer happy? (time, money, energy, etc.)
- What results do my customer expect? Which ones can mesmerize them? (quality level, profits and gains, savings and improvements, etc.)
- What current solutions enchant my customer? (functionalities, performance, quality, etc.)
- What can make my customer's tasks easier? (lower learning curve, more services, lower costs, etc.)

5

PHOENIIX GA No. 101070586

- What positive consequences do my customers want? (power, status, acknowledgment, satisfaction, motivation, etc.)
- What is my customer looking for? (design, guarantees, specific features, functionality, etc.)
- How does my customer measure success and failure? (cost, performance, speed, quality, beauty, likes on social networks, etc.)
- What would increase my customer's chances of adopting a solution? (lower investment, longer guarantee, better performance/quality/design, etc.)

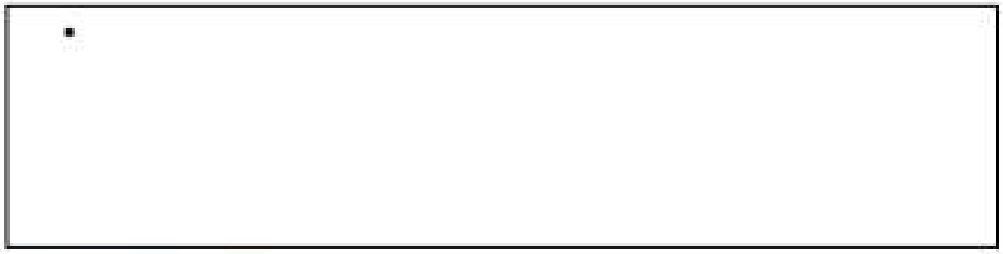


1.5.2.3 Pains

Guidance:

Pains encompasses everything that annoys your customer while they are performing their jobs-to-be-done, such as negative experiences and emotions, challenges, risks involved, financial costs, mistakes, and consequences, etc. Remember to classify each pain as severe or light and note down how often it takes place as well. To complete this step, you can make some questions:

- What is expensive for my customer? (regarding time, cost, effort, etc.)
- What makes my customer feel bad? (frustrations, disappointments, failures, physical pain, etc.)
- What are the main difficulties and challenges of my customer's faces? (physical, intellectual or emotional limitations to do something, resistance, understanding certain situations, etc.)
- How current solutions are leaving to be desired for my customer? (bad performance, much effort, lack of functionality, defects, etc.)
- What are the negative consequences for my customer? (losses of power, status, money, time, trust, etc.)
- What risks is my customer afraid of? (financial, social, technical, etc.)
- What is keeping my customer awake at night? (concerns, challenges, debts, bad health, etc.)
- What are the most common mistakes my customer makes? (creating expectations, misunderstandings, errors in use, etc.)
- What is preventing my customer from adopting solutions? (investment, learning curve, resistance to changes, etc.)



1.5.3 Value Proposition

1.5.3.1 Gain Creators

Guidance:

Gain creators involve how the product/service offers the customer added value, what are the benefits your product brings, and if your customer's wishes and expectations are reached. After all, how it makes your customer happier. Again, you should rank every gain your product or service creates according to relevance to your customers (if substantial or insignificant) and indicate how often it occurs. To do that, ask if your product/service:

- creates savings that make your customer happy (in terms of time, money, effort, etc.);

PHOENIIX GA No. 101070586

About each one, ask yourself:

- Can the product/service help to accomplish any job-to-be-done, whether functional, social, emotional, needs, wishes, roles, etc.?
- Is the product/service tangible, digital/virtual, or financial?
- Is the product/service crucial or trivial? How relevant is it?
- How often is the product/service used by my customer?