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

D6.2: Final Report on Dissemination, Exploitation, Standardisation & Sustainability

Abstract: This document represents a final report on activities performed by the PHOENIIX project on dissemination, exploitation, standardization & sustainability, within the second 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 & stakeholder engagement). Several key achievements of the consortium within the second 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, to the efforts related to the contribution in existing standardization activities, the identification of exploitable assets and a draft version of exploitation plan for the PHOENI2X solution / service. The document concludes with the presentation of activities and results from stakeholder engagement activities.

Contractual Date of Delivery	30.06.2025
Actual Date of Delivery	30.06.2025
Deliverable Security Class	PU - Public
Editor	Karras Apostolos (APS)
Contributors	UPAT, SANL, UPC, COSMOTE, FGC, PPC, WSE, AEGIS, SEA, EUNOMIA, ATOS, NODALPOINT, UiO, NCSA, DSA
Quality Assurance	EUNL, UiO

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: UNIVERSITETET I OSLO (UiO)

Reviewer #2: EUNOMIA LIMITED (EUNL)

Revisions

Version	Date	By	Overview
0.1	16/04/2025	APS	Document Template ToC
0.2	21/05/2025	UPC	Incorporated information on Dissemination and Communication
0.3	26/05/2025	COSMOTE	Incorporated information on Stakeholder engagement and liaison activities
0.4	30/05/2025	UPC	Updated content on communication and dissemination
0.5	01/06/2025	APS, COSMOTE	Updated content on exploitation, standardization and stakeholder results
0.6	17/06/2025	EUNL, UiO	Comments – QA review
0.7	24/06/2025	APS	Version incorporating comments
1.0	30/06/2025	APS	Final Version

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AI	Artificial Intelligence
BC	Business Continuity
CACAO	Collaborative Automated Course of Action Operations
CERT-EU	Computer Emergency Response Team for the EU institutions
CR	Cyber Range
CRC	Cyber Resilience Centre
CSIRTs	Computer Security Incident Response Teams
CTI	Cyber Threat Intelligence
CTI TC	Cyber Threat Intelligence Technical Committee
DAST	Dynamic Application Security Testing
DLMS/COSEM	Device Language Message Specification / Companion Specification for Energy Metering
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
FFNN	Feed Forward Neural Network
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
IR	Incident Response
ISACs	Information Sharing and Analysis Centres
ISO	International Organization for Standardization
KER	Key Exploitable Result
LSTM	Long Short-Term Memory
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
MS	Member State
NIS2	Directive on Security of Network and Information Systems - second version
OASIS	Organization for the Advancement of Structured Information Standards
OCA	Open Cybersecurity Alliance
OES	Operators of Essential Services
OWASP	Open Worldwide Application Security Project
RCR	Resilience Cyber Range
ROAR	Resilience Automation, Orchestration, and Response
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SDLC	Software Development Lifecycle
SOC	Security Operations Center
STIX	Structured Threat Information Expression
TAC TC	Threat Actor Context Technical Committee
TRL	Technology Readiness Level
UC	Use Case

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, Recovery 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 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, Cyber 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 reporting on the activities and outcomes of the second period of the project (M18-M36). 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. Stakeholder engagements and liaison activities, 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.

2 DISSEMINATION

This chapter provides a detailed overview of the communication and dissemination activities conducted during the second phase of the project. It also evaluates the associated Key Performance Indicators (KPIs). These activities include, but are not limited to, participation in events such as conferences and workshops, publication of scientific papers, blog posts, as well as other general outreach materials. Additionally, efforts to build relationships and foster synergies with related projects are highlighted.

2.1 Progress Highlights

2.1.1 Main achievements

During the second period of the project, the main achievements of PHOENI2X project in terms of communication and dissemination have been:

- Organization of two workshops (IOSEC 2024 and CyberHunt 2024) jointly with other EU-funded projects, achieving a total of 5 workshops organized.
- Co-sponsorship of two summer schools (CyberHOT 2024 and CyberHOT 2025) jointly with other EU-funded projects.
- Organization of two special issues: “Special Issue on Distributed Intelligence on the Internet” and “Special Issue New Challenges in Information Security and Privacy and Cyber Resilience”.
- Publication of a journal in the first quartile of the Journal Citations Report (JCR).
- Publication of six papers in International Conferences.
- Participation in 2 EU focused events, the 4th LETRA Learning & Training hands-on technical workshop and InnoTrans 2024.
- Participation in 5 technical, academic and industrial events, including the CyberHOT summer schools, 26th Infocom World conference Round Table: The need for the Digital Transformation Leap, Cybersecurity Risk Management and Governance in the Healthcare sector, Cybersecurity Risk Management and Governance in the Energy sector.
- Participation in 6 interactive face-to-face networking EU events, ETSI AI Conference Sophia Antipolis, CETEF’24, Intl Conference on the EU Cyber Security and Resilience Acts, REWIRE Infoday, DATAMITE and BEYOND.
- Collaboration with 19 EU-funded projects in the organization of International Workshops, summer schools and in the DATAMITE Meet Up event.
- Collaboration with OES stakeholders in the context of the Yearly Stakeholders Conference hosted at DSA’s premises.
- Collaboration with / contribution to cybersecurity policy makers e.g., ENISA ad-hoc working group on the European Cybersecurity Skills Framework (ECSF), 12th AHWG Plenary Meeting, Cybersecurity Awareness Training to Critical Information Infrastructures and Cyber security workshop with Ministry of Defense, Have your say activities.
- PHOENI2X increased the number of followers in LinkedIn to 125 new followers.
- The number of blog posts published during the second year of the project is more that 12, achieving a total number of 32 blog entries in the PHOENI2X website.

- 7 videos were published in the PHOENI2X YouTube and TikTok channels, as well as in the PHOENI2X social networks (LinkedIn and X).
- 3 Press releases and 4 Newsletters have been published during this last period of the project.

2.1.2 Key Performance Indicators

As outlined in the Grant Agreement, the consortium has defined a set of performance indicators to guide and evaluate the communication and dissemination activities throughout the entire duration of the project (see Table 1). These activities are closely monitored and coordinated by the designated task leader.

The performance indicators serve as key tools for assessing both the quantitative reach and the qualitative effectiveness of the actions undertaken. By regularly analyzing these metrics, the consortium can adapt its dissemination and communication strategy to ensure the achievement of expected outcomes and to enhance the project's visibility. This continuous monitoring enables a clear understanding of the overall impact and success of the communication efforts.

Table 1 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	Industry, OES,	Presentation material	≥8 flyers/brochures,

Channels	Target Audience	Activity/Measures	Measurable indicators and target value
activities	Policy makers		≥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 in D6.1 for monitoring the performance indicators, as listed in Table 2 and Table 3.

Table 2 PHOENI2X Dissemination Plan - KPIs

Activity/Measures	Targets				Expected Impact
	Y1	Y2	Y3	Total	
Journal publications	2 (2)	1 (2)	6[i] (4)	9[i]	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)	9 (6)	3 (7)	15	
Special issues/Book chapters	1[ii]-	- (2)	4[iii] (3)	5[iii]	
Workshops/Special sessions	2 (1)	1 (1)	2 (1)	5	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	2 (1)	7 (1)	14 (2)	23	
EU-focused event	-	-	2 (1)	2	Knowledge exchange with relevant communities and initiatives. Promotion of results to relevant communities and initiatives.
Technical, Academic, Industrial events	1 (1)	3 (1)	8 (1)	12	
Interactive face-to-face networking	-	5 (1)	5 (3)	10	Contact to external stakeholders to promote PHOENI2X solutions. Increased awareness.
Collaboration OES stakeholders	-	1 (-)	2 (3)	3	
Collaboration with cybersecurity policy makers	-	- (1)	5 (1)	5	

Numbers inside the parenthesis, indicate the target for each of the years of the project (Y1, Y2, Y3) whereas, the numbers outside the parenthesis, represent the achieved value for each KPI and year. The values in the column Total, represent the total value achieved for each KPI within the three years of the project.

[i] The project has published 4 journal publications during the lifetime of the project. Two more have been submitted and are currently under review. Three more will be submitted immediately after the project ends since they contain results from the validation. These have been counted within the KPIs in Table 2, Y3 and in the total figures and are presented in Section 2.2.1.1.

[ii] A review was performed on the dates of publication of the special issues / book chapters, and it was identified that one entry was mistakenly reported in Y2 instead of Y1. This mistake has been corrected in this table.

[iii] The project has participated in 5 special issues / book chapters during the lifetime of the project. The last of the journal special issues has been submitted and is currently under review, this last one has been counted within the KPIs in Table 2, Y3 and in the total figures and are presented in Section 2.2.1.3.

Table 3 PHOENI2X Communication Plan - KPIs

Activity/ Measures	Targets				Expected Impact
	Y1	Y2	Y3	Total	
Project website accesses	3228 (1000)	4125 (1000)	5668 (1000)	13021	Main online information channel. Communication of project news, events and results. Increased awareness.
Downloads	164 (100)	556 (100)	466 (100)	1186	
Blog posts	9 (9)	12 (12)	12[iv] (12)	32[iv]	
Twitter Followers	66 (50)	109 (75)	129 (100)	304	Attainment of interest of stakeholders active in social media. Sharing knowledge with other projects and initiatives. Drive engagement with the project.
Twitter Posts	52 (30)	104 (30)	48 (30)	204	
LinkedIn Connections	131 (100)	229 (150)	309 (200)	669	
Posts	46 (30)	64 (30)	42 (30)	152	
Facebook Followers	35 (35)	54 (50)	60 (100)	149	Attainment of interest of general public active in social media. Drive engagement with the project.
Posts	50 (30)	64 (30)	42 (30)	152	
Video clips	-	3(1)	4(1)	7	
Press releases	2(2)	2(2)	4[iv](4)	8[1v]	Promotion of results to relevant communities and initiatives. Proactive communications to the targeted stakeholders, the European Commission, researchers.
Newsletters	2(2)	2(2)	4[vi](4)	8[iv]	
Flyers/ Brochures	2(2)	1(3)	3(3)	6	Promotion of the project to stakeholders and scientific community. Attainment of interest. Drive engagement with the project.
Posters	1(1)	1(1)	1(1)	3	
General Public	-	1(1)	3(2)	4	Attainment of interest of general public. Drive engagement with the project.

[iv] The values in the Y3 columns (for blog posts, press releases, and newsletters), include also the last blog post, press release, and newsletter, that will communicate the end of the project. This deliverable was drafted before their publication, (which is scheduled to happen as soon as the project ends), but they are taken into account in both Y3 and the total values of Table 2.

In terms of dissemination KPIs, PHOENI2X has successfully met nearly all targets, particularly those related to international events, demonstrators, networking, and communication activities. Notable achievements include the co-organization of international workshops, active participation in technical, academic, and industrial events, engagement in EU-level networking, and collaboration with other projects, as well as with cybersecurity and policy makers**.** In terms of communication, web statistics and LinkedIn engagement are particularly noteworthy. The only KPI yet to be fulfilled is the number of journal publications, as the peer-review process for submitted papers is taking longer than expected. However, thanks to the project's final results, developed demonstrators, and strong

collaborative efforts, PHOENI2X is expected to produce a significant number of scientific publications after its completion. Currently, two more journal papers are in preparation.

In addition, as a result of the collaborative efforts within the project, five PHOENI2X partners have co-authored the book chapter titled "AI-Assisted Orchestration & Automation for Business Continuity, Incident Response & Information Exchange." This chapter will appear in an open-access book to be published by Springer. The book is a joint initiative involving several EU-funded projects in the fields of cybersecurity and cyber resilience.

2.1.3 Dissemination and communication plan beyond Y3

After the finalization of the project, on July 2025, there will still be outcomes of the project in the shape of scientific articles, events, webinars, etc. These outcomes should be still communicated/disseminated. For instance, three different papers have already been submitted:

- "Enhancing Cybersecurity in Railways: Machine Learning Approaches for Attack Detection" by Beatriz Otero, Eva Rodriguez, Juan Jose Costa and Mercedes Oriol, submitted to International Journal of Critical Infrastructure Protection.
- "Federated Transfer Learning-based Intrusion Detection System in 5G networks" by Andrea Bellmunt, Beatriz Otero and Eva Rodriguez, submitted to Engineering Applications of Artificial Intelligence.
- "A Machine Learning-Based Framework for Detection and Response to Cyberattacks in Critical Energy Infrastructures" by Raul Rabadan, Ayaz Hussain, Ester Simo, Eva Rodriguez and Xavier Masip, submitted to the Special Issue Multimodal Learning and Transfer Learning (Electronics Journal).

The book chapter titled "AI-Assisted Orchestration & Automation for Business Continuity, Incident Response & Information Exchange" in the open-access book Technology-Enabled Critical Infrastructure Resilience to be published by Springer.

In addition, other papers are now in process of development, most of them being the outcome of the collaboration between 2 or more partners.

On the other hand, PHOENI2X will co-organize the International Workshops, IOSEC 2025 and CyberHunt 2025. The 2025 IEEE CSR Workshop on Information and Operational Technology Security (IOSEC) will be held in Chania, Crete, Greece, on August 4–6, 2025, in conjunction with the 2025 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2025).

Apart from the outcomes after the end of the project, UPC will maintain the PHOENI2X website at least three years after the finalization of the project. UPC will be also in charge of PHOENI2X social media during this period after the lifetime of the project.

2.2 Dissemination activities

This section presents the dissemination activities conducted by the PHOENI2X partners in the second period of the project.

2.2.1 Scientific Publications

This section presents the scientific publications produced during the second period of the project, encompassing peer-reviewed journal articles, papers presented at international conferences, contributions to book chapters, and involvement in special issue editions.

2.2.1.1 Journal publications

During the second period of the project one journal paper has been published in the first Quartile of the Journal Citation Reports.

- ***A Differential Privacy protection-based federated deep learning framework to fog-embedded architectures.*** Gutiérrez, N., et al. (2024) Engineering Applications of Artificial Intelligence, 130 (2024): 107689, DOI: https://doi.org/10.1016/j.engappai.2023.107689. Open access. (JCR 7.4 Q1)

  Abstract: Nowadays, companies collect massive quantities of data to enhance their operations, often at the expense of sharing user sensible information. This data is widely used to train Deep Learning (DL) neural networks to model, classify, or recognize complex data. These activities enable companies to offer an array of services to users, such as precise advertising and optimal location services. This study explores potential solutions for preserving privacy while utilizing DL applications.

  To address the privacy issue, we develop a privacy-preserving framework specifically designed for fog computing environments. Unlike traditional cloud computing architectures, fog embedded architectures only share a small portion of user data with a nearby fog node, ensuring that the majority of sensitive data remains secure. Within these fog nodes, we incorporate two additional algorithms, namely Generalization and Threshold, to enhance the privacy-preserving capabilities of the framework.

  The first algorithm, Generalization, introduces a validation dataset within the fog nodes which not only increases the accuracy of the fog-embedded framework but also ensures that user data is preserved. The second algorithm, Threshold, is responsible for protecting user data samples and reducing the amount of information sent to the server. By combining these two algorithms, we are able to provide an additional layer of protection for user privacy while still maintaining the accuracy of the model.

  We conduct an evaluation to test its effectiveness using two separate datasets. In addition, we analyze them through a Feed Forward Neural Network (FFNN) and compare the results with a traditional centralized architecture to validate the effectiveness of the proposed framework.

  The results of our evaluation demonstrate that the proposed privacy-preserving framework, when combined with the Generalization and Threshold algorithms, can preserve up to 38.44% of user data. Additionally, we were able to extend the framework to multiple fog nodes without compromising the network's accuracy, as we only observed a 0.1% decrease in accuracy when using the proposed architecture.

  This study emphasizes the importance of preserving user information while using DL applications and provides a solution that trains the desired network without violating user privacy, hence preserving their anonymity. Overall, the study highlights the potential of Federated Deep Learning to improve the accuracy and privacy of DL applications in fog computing environments.

PHOENI2X partners also have submitted the following journals, currently under review:

- "Enhancing Cybersecurity in Railways: Machine Learning Approaches for Attack Detection" by Beatriz Otero, Eva Rodriguez, Juan Jose Costa and Mercedes Oriol, submitted to International Journal of Critical Infrastructure Protection.

- "Federated Transfer Learning-based Intrusion Detection System in 5G networks" by Andrea Bellmunt, Beatriz Otero and Eva Rodriguez, submitted to Engineering Applications of Artificial Intelligence.

PHOENI2X project partners are preparing to submit two more research papers for publication. One paper, focusing on honeypot technologies and their applications in cybersecurity, is intended for submission to the Journal of Information Security and Applications. The second paper, which presents research on the Threat Actor Context Ontology aimed at enhancing threat intelligence and adversary modeling, is being prepared for submission to ACM Computing Surveys. Finally, the third paper will present the overall results of the PHOENI2X project and will be submitted to IEEE Transactions on Dependable and Secure Computing.

2.2.1.2 Conferences

During the second period of the project 3 papers and 1 poster have been published in international conferences.

- ***A Deep Learning Framework for Safety Monitoring of a Railway Section.*** Chriki, F. Z. (2024). In IEEE International Conference on Cyber Security and Resilience (CSR), DOI: 10.1109/CSR61664.2024.10679387.
  Abstract: This paper presents an approach for anomaly detection and forecasting that aims to protect the integrity and operational continuity of IoT critical infrastructure, specifically for a railway use case. This system is designed to monitor in real-time the sensor data to detect any deviations that may indicate a potential data tampering attack or a sensor malfunction. This early identification and notification of such anomalies is crucial for preventing unauthorized access and mitigating the risks associated with data tampering attacks. The proposed system is comprised of two primary components: a forecasting component and an anomaly detection component. The Forecasting Component uses a Long Short-Term Memory (LSTM) model to predict future sensor values, while the Anomaly Detection Component employs the Tukey's fence method to identify sensor measurements that significantly deviate from normal behaviour. A railway use case is included to demonstrate the practical application of the deep learning framework. These components were evaluated and both demonstrated excellent performance. The Forecasting Component provided highly accurate predictions of future sensor values, while the Anomaly Detection Component effectively identified deviations from normal patterns. The evaluation results confirmed the system's ability to detect significant anomalies and its capability to maintain operational integrity and security in IoT critical infrastructures.

- ***Uncovering Hidden Threats: Automated, Machine Learning-based Discovery & Extraction of Cyber Threat Intelligence from Online Sources.*** *Ellinitakis, R. A. (2024).* In IEEE International Conference on Cyber Security and Resilience (CSR), DOI: 10.1109/CSR61664.2024.10679473.
  Abstract: The cyber-threat landscape is constantly and rapidly expanding, overwhelming human analysts in their effort to keep track of the latest threats. This affects both organisations that produce threat intelligence to be consumed by third parties, but also the end consumers of this threat intelligence, who want, for example, to configure proactive defences to protect their infrastructure. This paper presents a novel, Machine Learning-based, solution able to discover & ingest Cyber Threat Intelligence (CTI) data from unstructured online sources, such as dark web forums, social media and online chatrooms, producing a stream of standardised, structured STIX CTI data at its output. Further, a proof-of-concept is developed and assessed, to investigate its effectiveness with real-life data sources, but also to offer insights into the large amount of potentially useful threat intelligence -relevant information that lies unused in online sources, and the positive impact that the discovery and structuring

of this information in a standardised, easily shareable manner can have in terms of providing cyber defenders with an up-to-date and comprehensive view of the threat landscape.

- ***Towards Incident Response Orchestration and Automation for the Advanced Metering Infrastructure.*** Lekidis, A. (2024). In IEEE 20th International Conference on Factory Communication Systems (WFCS) , DOI: 10.1109/WFCS60972.2024.10540775.
  Abstract: The threat landscape of industrial infrastructures has expanded exponentially over the last few years. Such infrastructures include services such as the smart meter data exchange that should have real-time availability. Smart meters constitute the main component of the Advanced Metering Infrastructure, and their measurements are also used as historical data for forecasting the energy demand to avoid load peaks that could lead to blackouts within specific areas. Hence, a comprehensive Incident Response plan must be in place to ensure high service availability in case of cyber-attacks or operational errors. Currently, utility operators execute such plans mostly manually, requiring extensive time, effort, and domain expertise, and they are prone to human errors. In this paper, we present a method to provide an orchestrated and highly automated Incident Response plan targeting specific use cases and attack scenarios in the energy sector, including steps for preparedness, detection and analysis, containment, eradication, recovery, and post-incident activity through the use of playbooks. In particular, we use the OASIS Collaborative Automated Course of Action Operations (CACAO) standard to define highly automatable workflows in support of cyber security operations for the Advanced Metering Infrastructure. The proposed method is validated through an Advanced Metering Infrastructure testbed where the most prominent cyber-attacks are emulated, and playbooks are instantiated to ensure rapid response for the containment and eradication of the threat, business continuity on the smart meter data exchange service, and compliance with incident reporting requirements.

- ***Attacking the DLMS/COSEM Advanced Metering Infrastructure.*** *Accepted in 2025 IEEE CSR Workshop on Information and Operational Technology Security (IOSEC), August 4–6, 2025.*
  Abstract: The Device Language Message Specification / Companion Specification for Energy Metering (DLMS/COSEM) constitutes the de-facto communications backbone of contemporary Advanced Metering Infrastructure. As deployment density grows, so too does the protocol's exposed attack surface, warranting systematic scrutiny. This paper contributes a structured catalogue of DLMS/COSEM-specific cyber-attacks. After presenting the protocol stack and the AMI architecture, we develop a threat model spanning edge meters, field-area networks, and utility head-ends. We then describe 6 attacks, grouped into three attack classes: (i) False-Data Injection, (ii) Connection Disruption and Session Hijacking, (iii) Denial-of-Service at the application and network layers. The paper concludes by outlining research directions for detecting and mitigating these threats. Presents specific cyber-attacks to the DLMS/COSEM of Energy Infrastructure.

2.2.1.3 Special issues

During the second period of the project, PHOENI2X has participated in the organization of two special issues.

- ***ACM Transactions on Internet Technology - Special Issue on Distributed Intelligence on the Internet***[1]: *This special issue focuses on advancing the integration of diverse intelligent systems within next-generation Internet and IoT environments. Its purpose is to highlight how different types of intelligences, ranging from machine learning and automated planning to human input, can be interconnected to create semi-autonomous systems that evolve while keeping*

[1] https://dl.acm.org/pb-assets/static_journal_pages/toit/pdf/ACM-TOIT-CFP-DistIntInternet-1696149762410.pdf

humans actively involved. The issue aims to bring together both foundational research, such as architectures and interoperability of distributed intelligences, and practical applications involving real-world deployments. Emphasis is placed on the integration of heterogeneous intelligent systems and the role of human-AI collaboration across various sectors, with the ultimate goal of enabling more adaptive and intelligent Internet and IoT infrastructures.

- ***Special Issue New Challenges in Information Security and Privacy and Cyber Resilience, MDPI ElectroTnics***[2]***:*** *The objective of this Special Issue is to address the rapidly evolving landscape of digital threats by exploring innovative strategies to protect sensitive information, uphold privacy, and enhance organizational resilience against cyber incidents. In light of increasing technological complexity, interconnected devices, and cloud adoption, the issue examines emerging threats such as cyber-attacks, ransomware, and social engineering, while emphasizing the need for holistic security frameworks that balance protection with privacy rights. It seeks cutting-edge research on encryption, authentication, and access control, and places strong emphasis on cyber resilience, including preparation, response, recovery, and the role of human factors. Ultimately, the issue aims to bridge theoretical research and practical applications, fostering collaboration between academia and industry to empower cybersecurity professionals in safeguarding critical digital ecosystems.*

PHOENI2X partners are participating in the publication of the following book chapter.

- The book chapter titled "AI-Assisted Orchestration & Automation for Business Continuity, Incident Response & Information Exchange" in the open-access book Technology-Enabled Critical Infrastructure Resilience to be published by Springer.

PHOENI2X partners also have submitted the following papers in a journal special issue, currently under review:

- "A Machine Learning-Based Framework for Detection and Response to Cyberattacks in Critical Energy Infrastructures" by Raul Rabadan, Ayaz Hussain, Ester Simo, Eva Rodriguez and Xavier Masip, submitted to the Special Issue Multimodal Learning and Transfer Learning (Electronics Journal).

2.2.2 International Events

During the second reporting period, PHOENI2X co-organized two workshops contributing actively to knowledge exchange and community engagement. Additionally, the project is set to participate in the organization of another two workshops, IOSEC 2025 and CyberHunt 2025, following its official conclusion, further extending its impact and fostering continued collaboration within the research and innovation community.

IOSEC 2024

On September 4, 2024, PHOENI2X co-organized the IEEE CSR Workshop on Information and Operational Technology Security (IOSEC2024)[3] held in London, in conjunction with the 2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2024). The workshop has been organized jointly with the EU-funded projects JCOP, CUSTODES, CONSOLE, SYNAPSE and NGSOC. Chaired by the University of Patras (see Figure 1), the Workshop brought together more than 40 experts from diverse fields to explore common security challenges and solutions, aiming to advance the collective science and practice of IT and OT security. Topics covered included security architectures

[2] https://www.mdpi.com/journal/electronics/special_issues/Information_Security
[3] https://www.ieee-csr.org/archive/2024/iosec/index.html

and frameworks for critical infrastructures, threat modelling, AI in cybersecurity, vulnerability risk assessment and management, i Intrusion detection and prevention, and privacy enhancing technologies. A joint paper, from UPC and Worldsensing, entitled “A Deep Learning Framework for Safety Monitoring of a Railway Section” was presented at the workshop.

Figure 1: IEEE CSR Workshop on Information and Operational Technology Security (IOSEC2024)

Cyber Hunt 2024

The PHOENI2X project has co-sponsored (see Figure 2) the 7th Workshop on Cyber Threat Intelligence and Hunting (CyberHunt2024) in conjunction with the 2024 IEEE International Conference on Big Data (IEEE BigData 2024) held on December 18, 2024, PHOENI2Xin Washington DC, USA. This workshop brought together experts from academia, industry, and government to discuss advances on the domain of Cyber Threat Intelligence and other cybersecurity areas supported by the use of CTI.

Figure 2: 7th Workshop on Cyber Threat Intelligence and Hunting (CyberHunt2024)

PHOENI2X is co-organizing the 2025 IEEE CSR Workshop on Information and Operational Technology Security (IOSEC), that will be held in conjunction with the IEEE CSR 2025 conference the August 5,

2025, in Chania, Crete, Greece. This workshop (see Figure 3), will bring together perspectives from diverse domains to explore shared challenges and solutions in IT and OT security, with the goal of advancing both the science and practical application of cybersecurity across these environments.

Figure 3: IEEE CSR Workshop on Information and Operational Technology Security (IOSEC2025)

2.2.3 Demonstrators

PHOENI2X partners actively participated in a diverse range of events throughout the second phase of the project. These included demonstrators showcasing key technological advancements and use-case implementations, as well as high-level engagements with policymakers at both national and EU levels to discuss regulatory alignment and cybersecurity strategies. The consortium also contributed to EU-focused events, as well as to technical workshops, academic conferences, and industrial forums, ranging from webinars to hands-on training sessions, where PHOENI2X results were disseminated, and feedback from stakeholders was gathered.

2.2.3.1 EU-focused events

This section presents the EU-focused events where PHOENI2X partners have participated, fostering dialogue on emerging challenges and opportunities in the digital security domain.

4th LETRA Learning & Training hands-on technical workshop

Vasileios Mavroeidis, from the University of Oslo, participated in the 4th LETRA Learning & Training hands-on technical workshop focused on Incident Response and Defense Against Adversarial Actions, see Figure 4. Vasileios presented the CACAO business continuity playbook for the energy pilot developed in the PHOENI2X project regarding automation and orchestration.

Figure 4: 4th LETRA Learning & Training hands-on technical workshop

InnoTrans 2024

SANL participated in InnoTrans 2024[4], held in Berlin from September 24 to 27, where the European Commission, the European Union Agency for Railways, and Europe's Rail Joint Undertaking joined forces to showcase cutting-edge rail innovations. The joint stand featured a series of events highlighting advancements in the sector, including the Women in Rail awards, which celebrated outstanding contributions and achievements by women in the rail industry.

2.2.3.2 Technical, academic and industrial events

PHOENI2X has participated in technical, academic and industrial events. Additionally, PHOENI2X has co-sponsored two summer schools, and organized three training events.

CyberHOT 2024

PHOENI2X has co-sponsored the 4th Cybersecurity Hands -On -Training (CyberHOT) Summer School[5], which was organized in Piraeus, Greece, on Monday 9th and Tuesday 10th of September 2024, under the auspices of the University of Piraeus, Research Centre (UPRC). The CyberHOT Summer school sessions addressed the research of vulnerabilities of known components, the exploitation of existing vulnerabilities and privilege elevation on compromised targets. The CyberHOT Summer School has been jointly sponsored by the EU funded projects (see Figure 5): PHOENI2X, CyberSecPro[6], SENTINEL[7], CYRENE[8], IntelliIoT[9], EnerMan[10], SecOPERA[11], JCOP, REWIRE[12] and EDGELES[13].

[4] https://transport.ec.europa.eu/news-events/main-events/innotrans-2024_en
[5] https://www.cyberhot.eu/
[6] https://www.cybersecpro-project.eu/
[7] https://sentinel-project.eu/
[8] https://www.cyrene.eu/
[9] https://intelliot.eu/
[10] https://enerman-h2020.eu/
[11] https://secopera.eu/
[12] https://rewireproject.eu/
[13] https://edgeless-project.eu/

Figure 5: CyberHOT 2024 Summer School

CyberHot 2025

PHOENI2X co-sponsored the 5th Cybersecurity Hands-On Training (CyberHOT) Summer School[14], held in Chania, Crete, Greece, from May 26–30, 2025, under the auspices of the Technical University of Crete (TUC).

CyberHOT is an international training program that brings together experts from around the world to enhance technical skills in various areas of cybersecurity, including ethical hacking, risk management, incident response, and sector-specific cybersecurity challenges in the maritime, healthcare, and energy sectors.

This year, Alejandro Quintanar and Sebastian Pape from Social Engineering Academy (SEA) GmbH represented the PHOENI2X project at the summer school (see Figure 6). They organized a session on the HATCH serious game, designed to raise awareness and improve knowledge about social engineering attacks, showcasing the energy scenario as part of the game.

Figure 6: CyberHOT 2025 Summer School

26th InfoCom World conference

The PHOENI2X Project has been presented in the 26th InfoCom World Conference[15] "Digital Greece: Time for a Leap!" (see Figure 7) on November 12, 2024. The conference brought together experts from the fields of Information Technology and Telecommunications. Discussions revolved around private networks, artificial intelligence, data centres, e-government, smart cities and digital projects, giving special attention to the practical application and benefits of new technologies.

[14] https://www.cyberhot.eu/
[15] https://infocomworld.gr/en/

Figure 7: 26th InfoCom World conference

Cybersecurity Risk Management and Governance for Critical Infrastructures: Specialized Seminars in Energy and Health

APIRO has participated in the education and training initiatives in cybersecurity for Critical Infrastructure Operators[16], organized by the Digital Security Authority. As part of these efforts, two specialized seminars were held on December 17 and 18, 2024, at the Academy of Technology, Informatics, and Communications of the Office of the Commissioner of Communications. The seminars brought together designated information and network security officers from various Critical Infrastructures, aiming to enhance security practices in key sectors such as Energy and Health. APIRO's involvement contributed to the broader objective of strengthening sector-specific cybersecurity measures. The sessions addressed critical standards, including "ISO/IEC 27019 – Information security controls for the energy utility industry," focusing on the Energy Sector's unique cybersecurity needs, and "ISO 27799 – Health informatics: Information security management in health using ISO/IEC 27002," which outlines technical and organizational safeguards for the Health Sector.

PHOENI2X Internal training event – Energy use case

On Friday, June 20th 2025, the PHOENI2X Platform training workshop took place for the employes of the Energy Critical Infrastructure (PPC, Use Case 1). The total number of the workshop's participants was 15 of which 60% were IT/OT professionals and the rest 40% were generic personnel (see Figure 8).

The trainees had the opportunity to use the two training platforms that consist of the PHOENI2X solution:

1. SPHYNX Cyber Range (By SPHYNX Analytics S.A.), that focuses on cyber range training
2. PROTECT (by Social Engineering Academy GmbH) that focus on Serious games.

The training courses were separated into three categories:

Category #1: Training that focuses on IT/OT professionals working on the energy sector, delivered by the Sphynx CR: "Detection of DLMS/COSEM Attacks" and NIS2 Training for the Energy Sector.

[16] https://www.dsa.cy/category/news/energy-health-workshop

Category #2: Generic cybersecurity training for professionals, not confined in IT/OT and energy, delivered by the Sphynx CR: Cyber-hygiene training, GDPR training.

Category #3: Serious games, delivered by PROTECT, Cybersecurity Awareness, PROTECT for Administrative Personnel, PROTECT for IT/OT Professionals on the Energy Sector, PROTECT for Cybersecurity Experts (Business Continuity).

The workshop concluded with useful and positive feedback from the trainees over the training structure.

Figure 8: PHOENI2X Internal training event – Energy use case

PHOENI2X Internal training event – Transport use case

Within the framework of the PHOENI2X project, a cybersecurity training session was held on Monday 2 June at FGC's headquarters in Barcelona for railway control centre (CC) operators and members of the company. The training was prepared by the FGC team directly involved in the PHOENI2X project, together with the internal cybersecurity team.

The session lasted approximately 1 hour, and presented the main definitions, hardware elements, European and Spanish regulations and standards, and procedures to be taken into account by the CC operators in case of receiving, or suspecting, a cyber-attack to the critical infrastructure.

The training had the direct participation of 9 people in person, and 2 connected online, see Figure 8, taking a questionnaire at the beginning and end of the session to see the evolution of their knowledge of cybersecurity once they had attended the course.

Figure 8: PHOENI2X Internal training event – Transport use case

PHOENI2X Internal training event – Health use case

Two cybersecurity courses and one training event were held on June 23 and 27 in Athens, Greece, with eight participants from NODALPOINT attending, see Figure 9.

The Supply Chain Attacks course explores how cyber threats exploit trusted third-party software, services, and development pipelines to compromise systems. It introduces supply chain attacks with real-world examples like SolarWinds, Log4j, and Codecov, illustrating the severe impact of exploiting dependencies and update mechanisms. The course analyzes key attack vectors such as dependency confusion, typosquatting, CI/CD pipeline compromises, and third-party software risks, emphasizing how attackers leverage trust to infiltrate systems unnoticed. To counter these threats, it recommends best practices including vendor security audits, Software Bill of Materials (SBOM), code signing, secure dependency management, Zero Trust principles, and continuous monitoring. Collectively, these modules highlight the importance of proactive and layered defenses to secure the modern software supply chain.

The Secure Coding course equips developers and organizations with the knowledge to defend against supply chain attacks through secure software development practices. It underscores the importance of following OWASP Top 10 guidelines, validating user inputs, managing dependencies securely, and safeguarding authentication mechanisms. By integrating security throughout the Software Development Lifecycle (SDLC) and adopting DevSecOps practices, the course promotes early vulnerability detection via automated tools such as SAST, DAST, and SCA. It also covers regulatory compliance, examining frameworks like NIST, ISO 27001, the EU Cyber Resilience Act, and GDPR, and their requirements for secure development and vendor risk management. Finally, the course details a structured incident response process—from preparation to post-incident improvement—emphasizing the need for real-time detection, coordinated response, and continuous enhancement of security posture.

The NIS2 Regulatory and Compliance Training for the Healthcare Sector equips participants with a foundational understanding of cybersecurity obligations under the EU NIS2 Directive, tailored specifically to healthcare organizations. The course outlines which entities, such as large public and private hospitals and national laboratories, qualify as “Essential Entities” under NIS2. It emphasizes major threats—including unauthorized tampering with IoT medical devices and risks introduced by third-party vendors—and details best practices such as multi-factor authentication, regular risk assessments, and robust incident response strategies. The training also covers SOC (Security Operations Center) responsibilities like monitoring critical clinical systems, enforcing regulatory reporting timelines (e.g., 24-hour notification windows), and ensuring compliance of third-party providers. Practical scenarios highlight how SOCs should isolate compromised systems, activate response protocols, and manage legacy device risks without violating operational or budgetary constraints. The course integrates technical, procedural, and regulatory aspects to build cybersecurity resilience and operational continuity in healthcare environments under NIS2.

Figure 9: PHOENI2X Internal training event – Health use case

2.2.4 Networking/Outreach

This section outlines the EU events attended by PHOENI2X partners during the second phase of the project, highlighting their active participation in interactive, face-to-face networking.

2.2.4.1 Academics, Researchers, Industry

This section provides an overview of the conferences attended by PHOENI2X partners during the second phase of the project, where they presented scientific work and research outcomes achieved as part of the project.

ETSI Artificial Intelligence (AI) Conference

Eunomia Limited has participated at the ETSI AI Conference: Status, Implementation and Way Forward of AI Standardization, which was held from 5-7 February 2024 in Sophia Antipolis[17], France, presenting the poster "Standardization: AI Act's Cornerstone (see Figure 9). The conference discussed how Europe is addressing policy and legislation that will impact the deployment of AI, with particular attention to ensuring that AI systems placed on the EU market comply with existing laws on fundamental rights and EU values, and to facilitating the development of a single market for lawful, safe, and trustworthy AI applications. Eunomia's presentation focused on the significance of standardization for the implementation of the AI ACT and the ethical and legal challenges of AI standardization, also highlighting PHOENI2X's commitment to participating in standardization initiatives, especially in areas like AI- driven Cyber Security Tools

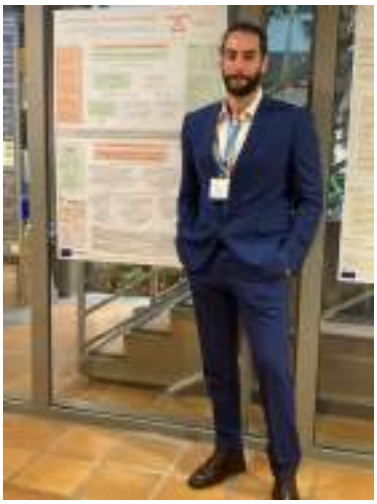


Figure 9: ETSI AI Conference

Central European Technology Forum

SANL participated in the CETEF'24[18], a major international forum organized by the Polish Chamber of Commerce for High Technology (IZTECH), under the patronage of the European Parliament and with the support of the European Commission. Co-organized with the AGH University of Science and Technology in Kraków, the third edition of the Forum brought together over 1,000 participants, including technology providers, end-users, research institutions, engineering associations, government bodies, financial institutions, and key EU policymakers. The event offered an excellent opportunity for SANL to present the PHOENI2X Project and to engage in networking and partnership-building aimed at shaping the future of Europe's high-tech landscape.

[17] https://www.etsi.org/events/2277-etsi-artificial-intelligence-conference
[18] https://cetef.eu/en/main/

Intl Conference on the EU Cyber Security and Resilience Acts

The University of Oslo has participated in the Intl Conference on the EU Cyber Security and Resilience Acts[19], held on March 11 to 13, 2024, in Brussels, Belgium. This conference is a prominent annual event that convenes cybersecurity professionals, policymakers, and industry leaders to discuss the implementation and impact of the EU Cybersecurity Act (CSA) and the Cyber Resilience Act (CRA).

REWIRE Infoday

The National Cyber Security Authority (NCSA) has participated in the REWIRE Infoday[20], held on April 23, 2024. This event was organized by the EU-funded project REWIRE, which aims to address the evolving challenges in the cybersecurity workforce across Europe. During the event, NCSA participated in the discussions surrounding the growing cybersecurity skills gap, a critical issue impacting both public and private sector organizations. They emphasized the urgent need for coordinated efforts to upskill professionals and build a more resilient digital infrastructure. NCSA's presentation focused on the skills gap in cybersecurity and how PHOENI2X project contributes in boosting the skills of professionals and enhancing the resiliency of organisations.

DATAMITE

PPC recently participated in the DATAMITE[21] Meet Up event engaging with stakeholders involved in the development of cutting-edge data management solutions, held on February 6, 2025. DATAMITE, a Horizon Europe project, delivers a modular, open-source, and multi-domain framework aimed at enhancing data monetization, interoperability, trading, and exchange. Through a combination of software modules, training resources, and business materials, the project seeks to empower European companies to establish themselves as key players in the evolving data economy. During the event, PPC highlighted the relevance of PHOENI2X's outcomes to the energy sector, particularly in strengthening business continuity and incident response processes. More specifically, PPC discussed the PHOENI2X contribution in business continuity and incidence response processes in the energy sector with relevant cybersecurity projects.

BEYOND

APIRO has participated in the BEYOND[22] international exhibition of technology, innovation, and entrepreneurship, held on March 04-06, 2025. BEYOND stands as the premier international exhibition dedicated to showcasing cutting-edge advancements in technology, innovation, and entrepreneurship across Southeastern Europe, the Mediterranean, and the Middle East. During this high-profile event, the PHOENI2X project was prominently featured at the National Coordination Centre for Cybersecurity (NCC-CY) booth. Representing the project, APIRO engaged actively with a diverse range of visitors, offering in-depth presentations and discussions about PHOENI2X's objectives and its role in strengthening cybersecurity at a national and European level. To enhance visibility and outreach, APIRO also distributed printed flyers, providing attendees with tangible information and key insights into the project's impact and vision.

2.2.4.2 Liaison with other projects, initiatives & communities

During the second phase of the PHOENI2X project, the consortium actively collaborated with 16 EU-funded projects to co-organize a variety of events, including workshops, networking meetups, and

[19] https://eucyberact.org/
[20] https://rewireproject.eu/infoday-3/
[21] https://datamite-horizon.eu/
[22] https://www.beyond-expo.gr/

summer schools. These joint efforts aimed to foster knowledge exchange and strengthen synergies within the domains of cybersecurity, artificial intelligence, and business continuity.

PHOENI2X took a leading role in organizing two major workshops, IOSEC 2024 and IOSEC 2025, in close collaboration with other EU-funded initiatives. These workshops provided a platform for experts, researchers, and stakeholders to share insights, present findings, and explore emerging challenges in secure and resilient digital infrastructures.

In addition to workshops, PHOENI2X co-sponsored two summer schools alongside partner EU projects. These educational initiatives were designed to train early-career researchers and professionals in cutting-edge topics relevant to the project's objectives.

PHOENI2X participated in the DATAMITE Meet Up, an event hosted by the DATAMITE EU-funded project, contributing to discussions and activities focused on data management and interoperability.

Furthermore, the projects PHOENI2X, CyberSecDome and Synapse had the opportunity to exchange ideas and present their projects during two events: the HSBooster standardization event (see 4.3) and the Cluster Synergies Webinar. The latter involved the presentation and discussion of 9 different related projects.

A summary of all EU-funded projects with which PHOENI2X has co-organized events is presented in Table 4. These collaborations highlight the project's active role in building an interconnected research and innovation ecosystem across Europe.

Table 4 PHOENI2X liaisons with other projects

Project	**Event**
CONSENTIS	IOSEC2025
CONSOLE	IOSEC2025, IOSEC2024, CyberHOT2025, Cluster Synergies Webinar
CUSTODES	IOSEC2024, CyberHOT2024, CyberHOT2025, Cluster Synergies Webinar
CyberSecDome	IOSEC2024, Cluster Synergies Webinar, HSBooster event
CyberSecPro	CyberHOT 2024, CyberHOT 2025
CyberSynchrony	CyberHOT2025
DATAMITE	DATAMITE Meet Up event
fAith	CyberHOT 2024
EDGELES	CyberHOT 2024, CyberHOT 2025
Elastic	CyberHOT 2025
NERO	CyberHOT2025
NGSOC	IOSEC2025, IOSEC2024
PANDORA	CyberHOT 2025
SAND5G	IOSEC2024
SecOPERA	IOSEC2024, CYBERHOT 2024
Synapse	IOSEC2024, CyberHOT 2025, HSBooster event, Cluster Synergies Webinar
Cocyber	Cluster Synergies Webinar
SecAwarenessTruss	Cluster Synergies Webinar
CRACoWi	Cluster Synergies Webinar
CoEvolution	Cluster Synergies Webinar

2.2.4.3 Policy makers

This section presents the meetings held with Operators of Essential Services (OES) stakeholders, focusing on the exchange of insights related to cybersecurity challenges and collaborative solutions. Additionally, the section highlights the interactions with cybersecurity policymakers at both the

national and EU levels, emphasizing discussions around regulatory frameworks, alignment with EU directives, and strategic initiatives to enhance resilience across critical infrastructures.

4th Stakeholders Conference

The PHOENI2X project was presented in the 4th Stakeholder's Conference organized by the Commissioner of Communications of Cyprus - Digital Security Authority (DSA). The event was held at the ICTACADEMY of the Office of the Commissioner of Communications of Cyprus, on November 19, 2024. The conference was attended by more than 200 representatives from ministries and independent authorities of the Republic of Cyprus, national and private bodies of critical information infrastructures, academic institutions, businesses, as well as representatives of organizations and companies from abroad. Participants came mainly from the energy, transport, health, water supply, banking and financial services, electronic communications, digital infrastructure and government security sectors. The PHOENI2X project was discussed among participants and a special roll-up banner (see Figure 10) was displayed during the three-day conference. APIROPLUS Solutions Ltd., a partner of the consortium was also one of the organizations participating in the meeting

Figure 10: 4th Stakeholders Conference

Additionally, during the second period of the project, PHOENI2X partners actively engaged in a series of strategic meetings and events at both the European and national levels to contribute to the evolving cybersecurity landscape. Notably, representatives participated in the 12th Plenary Meeting of the ENISA ad-hoc working group on the European Cybersecurity Skills Framework (ECSF), held in Brussels on 21 November 2024. This engagement continued with an online session on 17 February 2025, where discussions centered around the evolving role of the Incident respondent, involving ENISA and other key stakeholders. At the national level, PHOENI2X maintained strong collaboration with authorities in Greece, Cyprus, and Spain. In Cyprus, participation in the 4th Cybersecurity Conference, held on 26 September 2024 under the auspices of the Digital Security Authority (DSA), allowed for valuable dialogue with national cybersecurity stakeholders. The consortium also contributed to Cybersecurity Awareness Month by delivering targeted cybersecurity training to Critical Information Infrastructure (CII) operators and organizing a workshop with the Ministry of Defense on 17 October 2024, reinforcing the project's commitment to operational resilience and policy alignment across multiple governance levels.

2.2.5 Conferences

This section provides an overview of the conferences attended by PHOENI2X partners during the second phase of the project, where they presented scientific work and research outcomes achieved as part of the project.

IEEE 20th International Conference on Factory Communication Systems (WFCS)

On April 17, 2024, UiO and SANL presented the paper "*Towards Incident Response Orchestration and Automation for the Advanced Metering Infrastructure*" in the 2024 IEEE 20th International Conference on Factory Communication Systems (WFCS)[23]. This paper presented the joint work conducted in the PHOENI2X project on the definition of a methodology to provide an orchestrated and highly automated Incident Response plan targeting specific use cases and attack scenarios in the energy sector.

Figure 11: IEEE 20th International Conference on Factory Communication Systems

IEEE CSR 2024

On September 4, 2024, two PHOENI2X project related papers were presented in the IEEE CSR Workshop on Information and Operational Technology Security (IOSEC2024) held in London, in conjunction with the 2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2024)[24].

The paper "*A Deep Learning Framework for Safety Monitoring of a Railway Section*" jointly elaborated by UPC and WSE presented the early detection framework developed for the transport use case.

The paper "*Uncovering Hidden Threats: Automated, Machine Learning-based Discovery & Extraction of Cyber Threat Intelligence from Online Sources*" presented by SANL illustrates the CTI Discovery & Analytics approach used in PHOENI2X.

PHOENI2X project was among the organizing projects for both IOSEC2024 and IOSEC2025 that will take place August 2025.

[23] https://wfcs24.inviteo.fr/
[24] https://www.ieee-csr.org/archive/2024/index.html

Figure 12: IEEE CSR Workshop on Information and Operational Technology Security

2.2.6 Events

This section presents all the events where PHOENI2X has been present in this second period of the project.

2.2.6.1 PHOENI2X dedicated events

During the last year of the project the PHENI2X project has organized 4 plenary meetings, see Figure 13, and 4 internal workshops.

- **PHOENI2X 5th Plenary Meeting** in Athens, Greece, January 24-25, 2024. The meeting was hosted by COSMOTE, and its main objectives were to finalise the integration of the PHOENI2X framework and to prepare the first review meeting of the project.
- **PHOENI2X 6th Plenary Meeting** in Barcelona, Spain, July 1-2, 2024. The meeting was hosted by Worldsensing, and its main objectives were to discuss the new requirements for the final version of the PHOENI2X framework and to define the objectives of the project in its final year.
- **PHOENI2X 7th Plenary Meeting** in Braunschweig, Germany, October 1-2, 2024. The meeting was hosted by AEGIS, and its main objectives were to discuss the status and next steps for the three pilots of the project, including the final definition of the workflows, the final integration of the PHOENI2X framework.
- **NIS2 Directive National Cybersecurity Authority and basic organizations obligations:** An internal on-line workshop was held on November 13, 2024, during which the National Authority, NCSA, Ministry of Digital Governance, presented the NIS2 Directive to the whole PHOENI2X consortium. The session focused on the responsibilities and obligations of National Cybersecurity Authorities and key organizations under the directive, providing valuable insights into its implications for cybersecurity practices and compliance.
- **PHOENI2X 8th Plenary Meeting** in Madrid, Spain, February 25-26, 2025. The meeting was hosted by ATOS, and its main objectives were to finalise the integrations of the different components of the PHOENI2X framework and final steps for the three pilots of the project, including the validation and testing.
- **PHOENI2X 9th Plenary Meeting** in Nicosia, Cyprus, 10-11 JUNE 2025. The meeting was hosted by DSA, and its main objectives were to finalise the validation and testing activities for the PHOENI2X framework in the context of the three use cases of the project, as well as to prepare the consortium for the final review of the project.

Figure 13: PHOENI2X Plenary meetings

2.2.6.2 Other events

During the last year of the project the PHOENI2X project participated in the Cluster Synergies Webinar as indicated in the figure below.

Agenda

Time (CEST)	Project	Presenter
10:00 - 10:10	Welcome & Introduction	Vina Rompoti - ITML
10:10 - 10:20	CyberSecDome Project Presentation	Armend Duzha - Maggioli
10:20 - 10:30	COcyber Project Presentation	Alessandra Zini - EIT Digital
10:30 - 10:40	PHOENI2X Project Presentation	Argyro Chatzopoulou - Apiroplus
10:40 - 10:50	SecAwarenessTruss Project Presentation	Nikolaos Nikoloudakis - PPC
10:50–11:00	SYNAPSE Project Presentation	Panagiotis Bountakas - Sphynx
11:00–11:10	CUSTODES Project Presentation	Simon Bouget - RISE
11:10 -11:20	CONSOLE Project Presentation	Ciprian Pavel Oprisa - Bitdefender
11:20 -11:30	COevolution Project Presentation	Andreas Miaoudakis - CyberAlytics
11:30 - 11:40	CraCoWi Project Presentation	Chrysa Alexia - ITML
11:40 - 12:00	Q&A session	All

Figure 14: The Agenda of the Cluster Synergies Webinar

Figure 15: The 1st slide of the PHOENI2X project presentation within the Cluster Synergies Webinar[25]

Security and Privacy Workshop

UPAT held a workshop on privacy and security that was open to everyone, no technical background required. Throughout the event, the participants delved into a range of exciting initiatives, including the PHOENI2X Project, which explores new approaches to data protection and user consent in the digital age. It was a great opportunity to connect with a diverse audience, exchange ideas, and foster greater awareness around digital privacy. TEDx Patras provided the platform to join the workshop as depicted in Figure 18.

Figure 18: Security and Privacy Workshop

[25] Full presentation also available in video: https://youtu.be/Nm8l_1xeWDU

2.3 Communication activities

This section outlines the communication activities conducted in this second period of the project aimed at promoting project visibility and stakeholder engagement. It details the channels, tools, and strategies to ensure effective dissemination.

2.3.1 Website

As it has been reported in previous deliverables, the PHOENI2X website, https://PHOENI2X.eu/, is one of the main ways of communication. All the public content of PHOENI2X is made available on the website, such as blog posts, connection with the social networks, and newsletters also use the website as a place to point out.

During the final phase of the project, the PHOENI2X website (see Figure 16) has been consistently updated with the latest news, promotional materials, blog posts and newsletters. These updates have ensured that stakeholders, partners, and the wider public remain informed about the project's progress, key developments, and outcomes. The website has served as a dynamic communication hub, reflecting the project's ongoing activities and its contributions to innovation and collaboration in the cybersecurity and resilience domains.

Figure 16: PHOENI2X Web – main page

Figure 17 to Figure 23 shows the main statistics regarding the PHOENI2X website, for this second period of the project, from January 1, 2024, to June 3, 2025. In Figure 14, an interesting finding is the impact of the publications of the PHOENI2X Press Releases and Newsletters.

Figure 19 and Figure 20 show the most visited pages of the PHOENI2X website.

Finally, Figure 22 and Figure 23 show the top downloads, headed by the PHOENI2X Brochure, 3rd Newsletter, 1st Press Release, 4th Newsletter and 1st Newsletter.

Figure 17: PHOENI2X Visits statistics – second period of the project

Figure 18: PHOENI2X Web visitors map – last 90 days

Figure 19: Top pages – second period of the project

Figure 20: Top 5 pages – second period of the project

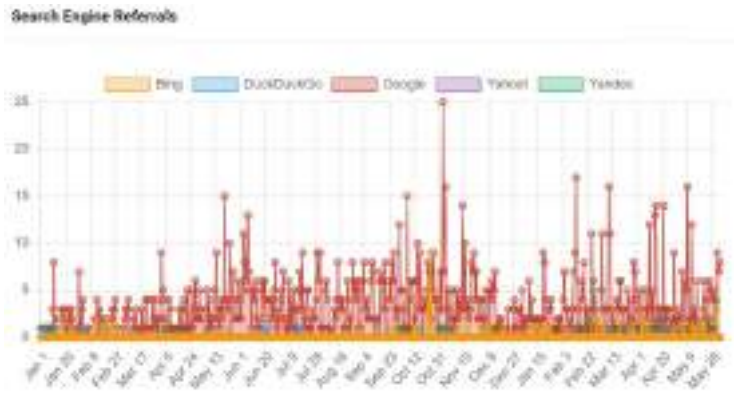


Figure 21: Search engines referrals

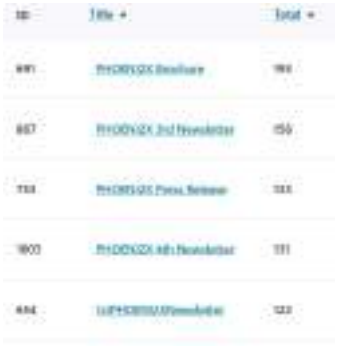


Figure 22: Top 5 downloads

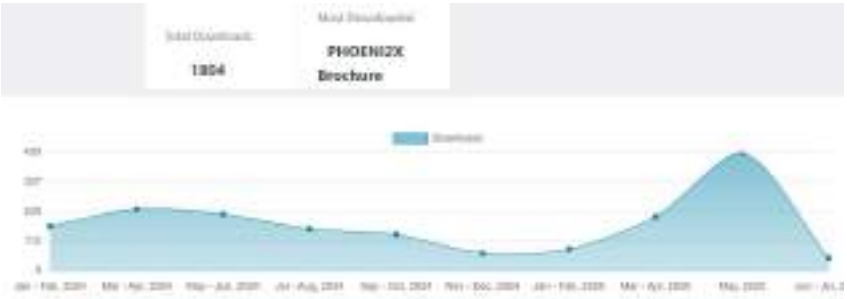


Figure 23: PHOENI2X downloads – second period of the project

2.3.2 Social Networks

Social media is used in the PHOENI2X project as a tool for disseminating research outcomes, project updates, and news to a wide audience. From the outset of the project, dedicated accounts were established on LinkedIn, Twitter (now X), and Facebook to ensure broad and effective communication.

Each platform is used to reach distinct segments of the target audience. Twitter is primarily aimed at the general public, but also to a wider community interested in innovation and technology, providing real-time updates and accessible insights into the project's progress. LinkedIn, on the other hand, targets a more professional and specialized audience, including researchers, industry partners, and other stakeholders in the scientific and technological domains. Facebook serves as an additional outreach channel, aiming to engage a broader and more diverse audience, including the general public and community groups, by sharing accessible content and fostering awareness of the project's goals and activities.

The data about these social networks on June 3rd, 2025, are:

- LinkedIn:
  - Link: https://www.linkedin.com/company/PHOENI2X/
  - Number of posts: 152
  - Number of followers: 309
- Twitter:
  - Link: https://twitter.com/PHOENI2XProject

  - Number of posts: 204
  - Followers: 129
- Facebook:
  - Link: https://www.facebook.com/PHOENI2X/
  - Number of posts: 156
  - Followers: 60

Figure 24 illustrates the most appreciated LinkedIn posts during the second phase of the project. The posts that garnered the highest number of impressions were primarily those related to the project's plenary meetings, highlighting the strong interest in key collaborative milestones. These were closely followed by posts about participation in external events, which also attracted significant engagement from the audience.

Figure 24: Most appreciated LinkedIn posts (June 3, 2025)

2.3.3 Video Clips

PHOENI2X maintains active YouTube[26] and TikTok[27] accounts as part of its outreach and dissemination strategy, as depicted in Figure 25. These platforms host a variety of video content aimed at both general and technical audiences. A general introductory video provides an overview of the project's objectives, scope, and impact. In addition, three dedicated videos, one for each of the project's use cases, highlight the specific benefits and real-world applications of the PHOENI2X framework in different critical sectors. To complement these, three more technically focused videos have been produced, showcasing key functionalities of the PHOENI2X framework. These videos offer deeper insights into important components of the PHOENI2X architecture, demonstrating how the framework has been implemented and validated within each use case. Together, these video resources serve to

[26] https://www.youtube.com/@PHOENI2XProject
[27] https://www.tiktok.com/@phoeni2xproject

increase public awareness, promote stakeholder engagement, and support the dissemination of technical achievements.

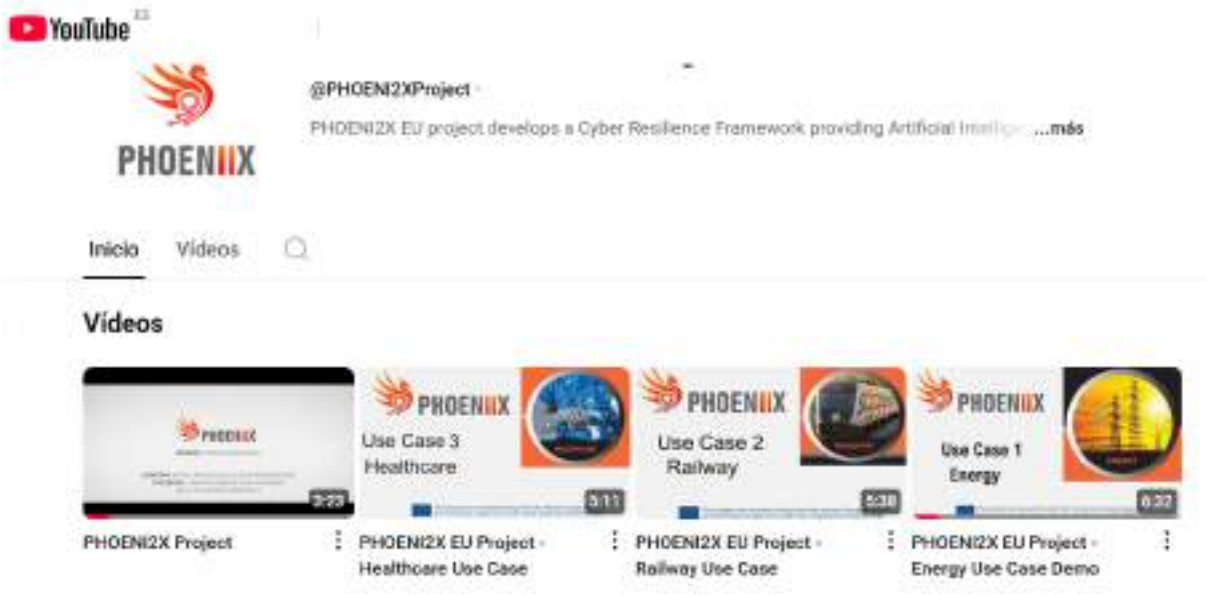


Figure 25: PHOENI2X YouTube channel

In addition to YouTube and TikTok, the videos have also been shared through the project's official LinkedIn and Twitter (now X) accounts to maximize visibility and engagement with a broader professional and policy-oriented audience. These platforms have been instrumental in reaching stakeholders from academia, industry, and public institutions, fostering interaction and raising awareness about the project's outcomes. By leveraging social media channels, PHOENI2X has strengthened its online presence and expanded the dissemination of its results beyond traditional channels.

As a result of these dissemination efforts, the videos have collectively reached 897 views across platforms, with particularly strong engagement on LinkedIn. This highlights the effectiveness of LinkedIn as a key channel for reaching the project's target audience, especially professionals and stakeholders in the cybersecurity, policy, and critical infrastructure domains.

2.3.4 Blog

The blog post strategy has been described both in the communication and dissemination project plan, as well as in D6.1. The idea of publishing a blog is to spread PHOENI2X to a more general audience and it is shared through a menu option in the Home page of the project website. PHOENI2X Blog posts are published on a monthly basis and are produced by all partners with a view to communicating project findings as well as igniting interesting conversations. Blogs are promoted in the social networks, LinkedIn, Twitter and Facebook. PHOENI2X blogs can be found in https://PHOENI2X.eu/blog/.

Figure 26: PHOENI2X Blog Posts

Table 5 shows the list of blog posts published during this second period of the project. During this period, PHOENI2X has published 17 blog posts. The blog posts covered topics related to specific enablers in the PHOENI2X framework, cybersecurity and cyber resilience in the project use cases related areas, PHOENI2X related standards, as well as PHOENI2X conducted Surveys.
At the end of June, the final blog post will be produced by PPC and published on PHOENI2X's social media channels.

Table 5 PHOENI2X Blog entries

Partner	Date	Title
PPC	January 2024	Elevating Cybersecurity in the Energy Sector: Insights from the PHOENI2X Project
FGC	February 2024	Cyber-attacks received in the railway sector
COSM	March 2024	Empowering Cybersecurity Excellence: OTE's Journey with PHOENI2X Innovations
UPAT	April 2024	AMINet: An Industrial Honeynet for AMI Systems
WOS	May 2024	Understanding and Mitigating Cybersecurity Risks in IoT Environments
SEA	June 2024	Overview of Social Engineering Attacks on PHOENI2X Use Cases and Novel Mitigations
EUNL	July 2024	EU's Cyber Resilience Act
SANL	August 2024	Achieving Cyber Resilience through standards-based, machine-processable & executable Incident Response & Business Continuity Playbooks
ATOS	September 2024	Leveraging CACAO Playbooks for Next-Generation Cyber Threat Intelligence and Response
UiO	October 2024	Towards Incident Response Orchestration and Automation for the Advanced Metering Infrastructure
NPS	November 2024	Backdoors and Breaches: How Supply Chain Attacks Threaten Healthcare and How to Fight Back
NCSA	December 2024	Building Intelligent SOCs for NIS2 Incident Reporting Requirements: A Strategy for Success
AEGIS	January 2025	The Role of Digital Forensics in Cyber Resilience: Insights from PHOENI2X
UPC	February 2025	Anomaly detection in railway infrastructures
DSA	March 2025	Building a Cyber Resilience Culture within Organizations
APS	April 2025	Mapping the Incident respondent: A Technical Perspective on Global Framework Diversity and the PHOENI2X Initiative
COSM	May 2025	Assessing PHOENI2X's Impactful Contribution to Cybersecurity Through Targeted Surveys

2.3.5 Newsletters

During the second phase of the project, four editions of the PHOENI2X Newsletter have been published. Each issue was carefully designed with specific communication objectives in mind, tailored to engage key audiences and highlight the progress of the project. In addition to showcasing major milestones and developments, the newsletters also featured key events, relevant news, and partner activities that took place during the respective periods.

These editions (see Figure 27) served not only as a tool for information dissemination but also as a strategic means of maintaining visibility, fostering stakeholder engagement, and promoting collaboration across the research community.

4th Newsletter
Date: March 2024

5th Newsletter
Date: July 2024

6th Newsletter
Date: November 2024

7th Newsletter
Date: April 2025

Figure 27: PHOENI2X Newsletters (second period of the project)

In June 2025, at the conclusion of the project, we will publish the final newsletter, highlighting our key achievements and recapping the most recent events attended by PHOENI2X partners.

2.3.6 Press releases

PHOENI2X press releases play a key role in promoting the project by communicating the benefits it offers to a wide range of stakeholders, including the general public, the scientific community, industry, and government bodies. Out of the eight planned press releases, three have already been published by the Use Case (UC) owners. During the first phase of the project, related UC owners press releases were issued by PCC and FGC. In the second phase, Nodalpoint, DSA, NCSA (see Figure 28) and WSE, took the lead in publishing additional releases. These communications have significantly enhanced the project's visibility, leading to increased engagement across our social media platforms and a noticeable rise in the visits to the PHOENI2X website.

Table 6 PHOENI2X Press Releases (Second period of the project)

# Press Release	Author	Date
4th Press Release	NODALPOINT	March 2024
5th Press Release	DSA	December 2024
6th Press Release	NCSA	May 2025
7th Press Release	WSE	June 2025

Figure 28: PHOENI2X 6th Press release

In June, Worldsensing will publish a PHOENI2X press release highlighting the final achievements of the transport use case. At the project's conclusion, a final press release will also be issued, showcasing the PHOENI2X framework and its validation across all three use cases.

2.3.7 Dissemination & communication toolkit

This section presents the printed/published online dissemination materials developed for the PHOENI2X project during the second reporting period. These materials, including brochures, posters, and infographics, are primarily used during face-to-face meetings and events to effectively communicate key aspects of the project. All items are freely accessible to partners via the PHOENI2X website and repository, ensuring wide availability and consistent messaging across dissemination activities.

2.3.7.1 Brochure

The main objective of the brochure is to provide our audiences with an engaging and well-written overview of the project, highlighting its key objectives and main features. During the second reporting period, four flyers and brochures, as depicted in Figure 29, were developed and distributed to support this goal. These materials were specifically designed to enhance the visibility and understanding of the PHOENI2X framework and its associated use cases. By visually summarizing complex information, they serve as effective tools for communicating the project's value to both technical and non-technical stakeholders during events, meetings, and outreach activities.

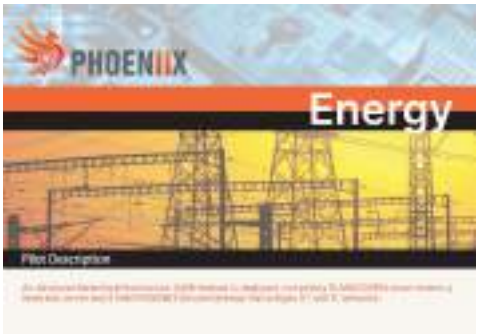


Figure 29: PHOENI2X brochures (second period of the project)

Two additional brochures will be prepared for the IOSEC 2025 workshop. The first will showcase the serious games developed within the PHOENI2X project, emphasizing their educational value and role in cybersecurity awareness and training. The second will highlight the key innovations of the PHOENI2X framework, providing a clear and accessible overview of its technical advancements and impact across the project's use cases.

2.3.7.2 Poster

During the first reporting period of the project, two posters were developed with the aim of capturing audience attention and providing a clear, concise overview of the PHOENI2X project. These posters served as effective visual tools at events and meetings, helping to quickly communicate the project's purpose and impact.

In the second reporting period, a dedicated poster was created specifically for presentation at the 26th InfoCom World Conference. This poster, shown in Figure 7, was tailored to the theme of the conference and strategically designed to highlight PHOENI2X's relevance in the context of Greece's digital transformation. It contributed to raising awareness among a broader audience, including industry professionals, policymakers, and researchers.

2.3.8 Media publications

During the second phase of the project, three news articles related to the PHOENI2X project were published across digital newspapers and partner websites, as shown in Figure 33.

Notably, on June 17, 2025, the Economy Today Cypriot newspaper featured a news article titled "APSA: Participation in the European PHOENI2X Project to Counter Cyber-Attacks." The piece highlights the Digital Security Authority's (DSA) involvement in PHOENI2X. DSA, as the Competent Authority for the Security of Network and Information Systems of the Republic of Cyprus, plays a key coordinating role, coordinating role in the project since it contributes to the supervision of the regulatory and technical aspects of the project, aiming at the development of a Directive (EU) 2022/2555 (NIS2) compliant platform, adapted to the needs of critical infrastructure operators.

NCSA published a news article titled “European project PHOENI2X: Strengthening the defence of critical infrastructure” on its website. The article emphasizes NCSA’s role as the competent national authority for the implementation of Directive 2022/2555 (NIS2 Directive), and in particular as a supervisory authority for the implementation of the requirements arising from it, is responsible for overseeing compliance with the regulatory framework, European and national, as a whole in the field of cybersecurity. H.A.K., by participating in the consortium of the PHOENI2X project, contributes to the dissemination of the project and the dissemination of its results. In addition, it will play an important role in validating the use of the platform in the Energy sector.

Finally, WSE published a news article “AI-based cyber robustness for transport operators” on its website. The article highlights WSE’s contributions to the project, with a focus on the development of technology for monitoring critical security parameters. It emphasizes the attention given to data security and integrity across the entire end-to-end IoT solution, as well as the cyber robustness of the operational technology (OT) software suite. This suite supports device and network management, alert generation, and data integration.

Figure 30: PHOENI2X in the news

3 EXPLOITATION

The primary objective of Task 6.2 is to establish a comprehensive exploitation framework that ensures the sustainability and impact of the PHOENI2X results, focusing on the identification, assessment, and valorisation of Key Exploitable Results (KERs). This includes the development of exploitation strategies for individual partners and the consortium, while incorporating intellectual property rights (IPR) considerations, market analysis, and alignment with standardization and policy-making efforts. The outcomes of Task 6.2 are intended to support both commercial and non-commercial uptake of the project outcomes.

More specifically, the task aims to:

- Identify and characterize the project's Key Exploitable Results.
- Develop and update individual and joint exploitation plans.
- Evaluate the market potential and innovation readiness of the KERs.
- Define and monitor appropriate IPR strategies.
- Lay the groundwork for post-project sustainability.

3.1 Progress Highlights

During the second period of the project, the main achievements of PHOENI2X project in terms of co-exploitation have been:

- Review of the KERs extracted during the first reporting period and re-affirmation of their importance and applicability.
- Drafting of an exploitation plan for the PHOENI2X service / solution (KER1).
- Definition of exploitation plans for the rest of the KERs.
- Identification and implementation of an IPR protection methodology.
- Extraction of results regarding the ownership of the KERs of the project.
- Definition of a commercialization strategy to be used after the end of the project.
- Definition of a post-project Business Plan and Marketing strategy.

3.2 Initial Exploitation Plan

During the first 18 months of the project, as reported in D6.1, an initial exploitation plan was established. Key activities included:

- The definition of an exploitation design methodology to guide partner inputs and evaluation processes.
- The collection of structured information from all partners on the exploitation potential of project outcomes, encompassing both the integrated PHOENI2X solution and its individual technological components.
- The identification and preliminary classification of the most prominent Key Exploitable Results (KERs) based on their innovation level and market relevance.
- The initial gathering of partner-specific exploitation intentions and potential pathways (e.g., commercial, academic, open source).

These preparatory activities laid the foundation for the more detailed validation, exploitation strategy refinement, and stakeholder engagement actions undertaken in the current reporting period, as described in the following sections.

3.3 Exploitation design methodology

The exploitation design methodology adopted by the PHOENI2X consortium (also described in details in D6.1) provides a structured approach for identifying, evaluating, and prioritising exploitable outcomes. It ensures that exploitation strategies are tailored to the characteristics of each Key Exploitable Result (KER) and aligned with the partners' expectations and capabilities.

The methodology consists of four main steps:

1. **Data Collection**
   Collection of structured information from partners regarding exploitable outcomes, ownership status, intended protection mechanisms (IPR strategies), and preliminary market opportunities. The input was gathered through a targeted exploitation and IPR questionnaire.
2. **Input Ranking**
   Development of ranking criteria, including technological readiness level (TRL), market attractiveness, innovation uniqueness, and strategic alignment. Each exploitable outcome was scored and prioritised based on these dimensions to identify those with the highest exploitation potential.
3. **Market Analysis**
   Evaluation of sectoral needs and market demands, assessing the relevance of the identified results against external expectations and trends in cybersecurity, resilience, and compliance.
4. **Definition of Exploitation Strategies**
   Definition of partner-specific and joint exploitation strategies, encompassing commercial, academic, open-source, and institutional pathways for each prioritised KER.

As a result of the application of this methodology, five (5) Key Exploitable Results (KERs) were identified during the first half of the project:

1. **PHOENI2X Solution** (comprehensive cyber resilience framework)**,**
2. **ROAR** (incident response tool)**,**
3. **CR** (Cyber Range tool)**,**
4. **TINTED** (CTI discovery, analytics, and threat hunting platform)**,**
5. **CP** (Compliance Process support tool)**.**

In line with best practices for exploitation management, a re-evaluation exercise was conducted in month M34. Partners were invited to update their inputs via the pre-existing questionnaires. Based on the updated data, the five KERs were reaffirmed, and IPR strategies were identified for each of them, paving the way for post-project exploitation.

It should be noted, that the KERs identified vary in type, ownership and approach, and as such the results extracted also from the next steps of the exploitation strategy of the project, differ. (e.g. the **PHOENI2X Solution** has been identified as a joined exploitable result and is a combination of services and tools, **TINTED** is a platform owned by only one partner and **CP** is a service)

3.4 Draft Exploitation Plan for KER 1

3.4.1 What is to be exploited

KER1 is the PHOENI2X Service / Solution. The PHOENI2X Service / Solution aims to bolster the cyber resilience of Operators of Essential Services (OES) across sectors such as energy, transport and healthcare. By integrating Artificial Intelligence (AI)–assisted orchestration, automation and response capabilities, the Service / Solution seeks to enhance business continuity, incident response and information exchange mechanisms thus improving cybersecurity in EU. The PHOENI2X Service / Solution is provided by combining and aligning different components. Due to this modality, the PHOENI2X Service / Solution can be customized and provided to each customer as needed based on their own needs. **PHOENI2X Resilience-as-a-Service (RaaS)** offers a **cutting-edge**, **modular cybersecurity service** designed to help Operators of Essential Services (OES) and EU Member State authorities enhance their **preparedness, detection, response, and recovery capabilities** in the face of evolving cyber and hybrid threats. Built on the PHOENI2X Cyber Resilience Framework, this service integrates AI-assisted automation, orchestration, and real-time threat intelligence to deliver comprehensive, scalable cyber resilience support.

3.4.2 Technology readiness level (TRL)

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, the solution / service was validated through three different use-cases, within a controlled environment. Based on the European definition of TRLs[28], that at the end of the project, the PHOENI2X Service / Solution will be at TRL 4 - technology validated in lab.

3.4.3 Target group and end users

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.

The target groups and end users of the PHOENI2X Service / Solution are depicted in Table 7. For each one of these groups, their specific interest on the service / solution is provided. The target groups identified are not only potential customers (buyers) of the service / solution but also entities that can exploit its results, insights or actions.

Table 7 Target groups and end users of the PHOENI2X Service / Solution

Type of Stakeholder	Interest
Critical infrastructure organizations (CIOs) (e.g. in energy, transportation, health domains) or in general, organizations with obligations stemming from regulatory frameworks such as GDPR, NIS2, eIDAS.	Potential customers / users of the PHOENI2X Service / Solution

[28] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Type of Stakeholder	Interest
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.	Potential customers / users of the PHOENI2X Service / Solution
Public Sector and Institutional Users	Indirectly interested in the PHOENI2X Service / Solution. They would be interested in using the system as they are identified as OESs based on NIS2.
Policy makers at any level (Ministries and Governments, other related European and national agencies, Standard Developing Organizations, etc.)	Interested in adopting the best practices related to incident response and business continuity play-books as well as the relevant communication taxonomy.
Academia and Research	Interested in gaining insights and building on top of the provided solutions.

3.4.4 Format

As mentioned above, PHOENI2X holistic approach integrates Prevention, Detection & Response via a fully-featured baseline toolset. This toolset comprises services (e.g. consulting, customization, training etc), cloud services (e.g. software that is deployed as a Service (SaaS)) and software that needs to be installed at the customer side.

This format of the PHOENI2X Service / Solution creates special issues that need to be resolved until full commercialization can be possible (as noted above, the PHOENI2X Service / Solution will reside at TRL 4 at the end of the project duration).

An overview of the possible issues:

- For the successful design, implementation and roll-out of the PHOENI2X Service / Solution, different entities have to collaborate.
- Each entity provides a different component of the PHOENI2X Service / Solution, at different percentages.
- Each entity has a different contribution to the formulation of the final implementation of the PHOENI2X Service / Solution in each customer, some of the contributions being intangible.
- Each entity resides at a different country, with different rules regarding commercialization, taxation and legal constraints and jurisdiction.

The project partners have extensively discussed on the above issues and have initially decided that the best available solution could be a Holding Company (Special Purpose Vehicle - SPV).

3.4.5 Expected outcome

The Holding Company (Special Purpose Vehicle - SPV), shall:

- Act as the commercial front for the PHOENI2X Service / Solution.
- Not own the IP of the components but will have the right to exploit them (under defined terms).
- Be a private limited company (e.g., GmbH, SARL, Ltd) established in an EU country, decided by the partners after careful examination.

- Provide a cloud service consisting of different components and manual services, for the customization to the customers' needs.

The key decisions / considerations that the PHOENI2X consortium will need to make in relation to the SPV are the following:

1. How will IPR regarding the individual components and the sum of the PHOENI2X Service / Solution be managed?
2. What kind of legal instrument (e.g. agreement) will be used in order to clearly define the allocation of IPR in every case per involved partner?
3. What will the role of each involved partner be, in relation to the different phases of the service (for example, will partners be involved in the promotion, advertisement, contact and contract management?)
4. What will the pricing model be (e.g. it could be API call-based, user-license based, etc.)?
5. How will revenue be shared between the involved entities (e.g. revenue pooling with proportionate distribution, or micro-payments per component usage etc)?
6. How will the SPV be managed and what will the governance structure be to allow for effective collaboration, transparency and efficiency?

Although at this point, all of the above questions cannot be answered, the project partners have implemented preliminary work in relation to the identification of IPR ownership between partners per component. The methodology and the results of this exercise are documented in Section 3.4.6.

3.4.6 Overview of SPV related activities

This section provides an overview of the steps that need to be followed in order to set up an SPV, that would be responsible for the exploitation and promotion of the PHOENI2X Service / Solution.

- **SPV Setup**
  A holding (or special purpose vehicle – SPV) is established in an EU country to market and operate the integrated service. The involved partners shall license their individual IP to this SPV, which sells, hosts, and maintains the system.
- **IP Ownership & Licensing**
  Each partner retains ownership of their individual components. They grant the SPV a license—non-exclusive or exclusive—specifying permitted use, territory, and duration.
- **Revenue Collection & Attribution**
  SPV centrally collects revenue (e.g., subscriptions, API fees). It uses **usage metrics** (like API calls or user sessions) and pre-agreed weightings to split revenues proportionally among partners each payment period.
- **Governance & Financial Flow**

  The SPV has a governance structure (board, voting rules). Activities and structure are implemented in order to ensure financial transparency, including regular reporting and audits as prescribed by the legal requirements of the country of establishment. The structure and the governance procedures of the SPV shall also define the way that the payments / payouts to the contributing partners will be implemented. The adopted method shall reflect the framework agreement between the partners.

- **Agreement Framework**
  A consortium agreement (or joint exploitation agreement) detailing the IPR licensing, the governance, the revenue model, the agreed method for dispute resolution, the exit mechanics and extension rules, shall be drafted and agreed between the involved partners.

3.5 IPR protection methodology

The PHOENI2X consortium adopted a structured and transparent approach for managing Intellectual Property Rights (IPR) associated with the project's Key Exploitable Results (KERs). Recognising the diversity of results in terms of ownership, protection strategies, and intended exploitation forms, a dedicated methodology was established to ensure clarity, fairness, and alignment among partners.

To systematically collect and validate information, an **IPR Questionnaire** was designed and distributed to all consortium members. The questionnaire captured structured input regarding:

- The name and description of the exploitable result,
- The type of result (e.g., service, software, process),
- Ownership status (individual or joint),
- Intended exploitation forms (commercial, open-source, institutional use),
- Preferred IPR protection mechanisms (e.g., copyright, licensing, open-source dissemination).

Table 8, presents the ownership of each identified KER. Two (2) of the identified KERs (PHOENI2X Service / Solution and CP Compliance Process) have been identified as having joined ownership and four (3) are identified as belonging exclusively to the one partner (2 to SANL and 1 to ATOS).

Table 8 Ownership of each identified KER

KER	Description	Owner
KER_01	PHOENI2X Service / Solution	Joined (see below)
KER_02	ROAR Incident Response tool	SANL (SPHYNX ANALYTICS LIMITED)
KER_03	CR Cyber Range tool	SANL (SPHYNX ANALYTICS LIMITED)
KER_04	Threat Intelligence Integrator (TII) or TINTED[29]	ATOS (ATOS IT SOLUTIONS AND SERVICES IBERIA SL)
KER_05	CP Compliance Process	Joined (see below)

The following sections provide an overview on the approach regarding IPR selected for each one of the KERs. For the KERs that are exclusively owned by one project partner, the decisions and approaches depicted in the respective sections, have been taken by the responsible partner. For the KERs that are jointly owned by more than one project partner, the decisions and approaches depicted in the respective sections, are the result of the collaborative efforts of the involved partners.

3.5.1 IPR Analysis of the PHOENI2X Service / Solution

As can be seen in Section 3.3.4.1 of Deliverable 6.1, the assessment for each key exploitable result was based on their technical maturity, market potential, target audience & market size, the major players, and the protection of the intellectual property rights.

From this analysis, the PHOENI2X Service / Solution was identified as having potential for exploitation, as the increasing digitalisation of modern organizations, along with the evolution of Artificial Intelligence, machine learning, and the Internet of Things among others, have led to a robust growth

[29] Previously called CTI Discovery Analytics & Threat Hunting (TII) TINTED

of the global cybersecurity market over the past few years, a growth that is expected to continue in the years to come.

To exploit the market potential of the PHOENI2X Service / Solution the following actions have taken place within the framework of the project as part of the PHOENI2X Service / Solution exploitation plan:

3.5.1.1 Allocation of ownership rights among partners

Given that the PHOENI2X Service / Solution is a consolidation of different tools, with services and solutions coming from different partners, the first step in formulating the PHOENI2X Service / Solution exploitation plan consisted in allocating the ownership rights among the project partners.

To assess the ownership rights of the different partners, each partner outlined their financial, intellectual, and resource contribution to the development of the PHOENI2X Service / Solution. The contribution of each partner is summarized in Table 9 below.

Table 9 Contribution of each partner in the development of the PHOENI2X Service / Solution

Partner	Contribution
UPAT	Provision of intrusion detection for industrial sector (energy smart meters)
SANL	Ownership and provision of the SPA, ROAR, RCR, and UEBA components
AEGIS	Provision of Forensics Visualisation Toolkit (FVT) component
ATOS	Provision of the CERCA, SMIR and TINTED components
NODALPOINT	Provision of the SCP Key Exploitable Result

To the information of Table 9, it should be noted, that other partners of the project, provided parts, infrastructure, knowledge as needed, although their contribution is more closely connected to either the pilot environment or have decided not to claim ownership on the final outcome.

Examples of these cases are: NODALPOINT, who provided also the infrastructure for the healthcare pilot, OTE who provided the fall-back solution for the energy use case and PPC who provided the Advanced Metering infrastructure testbed. These parts although crucial for the implementation of the pilots that facilitated the validation of the PHOENI2X Service / Solution, would not be needed for its further exploitation.

To summarize the above-mentioned information, the following table has been created.

Table 10 Classification of the contribution of each partner in the development of the PHOENI2X Service / Solution

Partner	Contribution Type	Description of Contribution
UPAT	Provision of parts/components	Provision of intrusion detection for industrial sector (energy smart meters)
SANL	Provision of parts/components	Ownership and provision of the SPA, ROAR, RCR, and UEBA components
AEGIS	Provision of parts/components	Provision of Forensics Visualisation Toolkit (FVT) component
ATOS	Provision of parts/components	Provision of the CERCA, SMIR and TINTED components
NODALPOINT	Provision of parts/components	Provision of the SCP Key Exploitable Result

Partner	Contribution Type	Description of Contribution
NODALPOINT	Provision of testbed	Provision of the infrastructure for the healthcare pilot.
OTE	Provision of testbed	Provision of the fall-back solution for the energy use case
PPC	Provision of testbed	Provision of the Advanced Metering infrastructure testbed

3.5.2 IP Protection Strategy and Ownership Type

Once the contribution of all partners in the development of the PHOENI2X Service / Solution has been identified, the next step in the exploitation plan consisted in selecting the appropriate intellectual property rights strategy and type of ownership.

Regarding the **IP protection strategies**, the following have been discussed among the partners:

1. **Filing Patents**: Ensure that inventions are patented to prevent unauthorized use.
2. **Registering Copyrights and Trademarks**: Officially register copyrights and trademarks to establish legal protection.
3. **Confidentiality Agreements:** Use non-disclosure agreements (NDAs) to protect trade secrets and sensitive information.
4. **Open source**

Regarding the IP ownership types, the following have been discussed among the partners:

1. **Joint Ownership**: Partners may agree to jointly own the IP, sharing rights and responsibilities.
2. **Exclusive Ownership**: One partner may own the IP exclusively, with others receiving licenses to use it.
3. **Proportional Ownership**: Ownership can be divided based on each partner's contribution to the project.

After considering all alternatives, the partners agreed that in the exploitation of the PHOENI2X Service / Solution, each partner contributing components/parts will employ its own IP protection strategy, and retain exclusive ownership of the intellectual property rights stemming from their contribution, except for UPAT, whose components will be used under an open-source status, as outlined in Table 11.

Table 11 Intellectual property rights protection strategy per partner

Partner	IPR Protection Strategy	IPR Ownership Type
UPAT	Open source	CC / Open source
SANL	For the SPA, ROAR, RCR, and UEBA components, SANL will adopt a comprehensive IP protection strategy by registering copyrights to secure legal ownership and enforceability. Additionally, SANL will ensure the protection of sensitive information by signing NDAs when sharing details with third parties (e.g., subcontractors or collaborative partners) during or after the project's implementation. Preliminary agreements on knowledge and IPR management will also be established with relevant parties as needed.	SANL retains exclusive ownership of all intellectual property rights related to the SPA, ROAR, RCR, and UEBA Key Exploitable Results. This ensures full control over the tools, including their use, distribution, and any modifications, while safeguarding sensitive information and enabling effective IP management

Partner	IPR Protection Strategy	IPR Ownership Type
AEGIS	AEGIS will reach preliminary agreements with relevant parties on knowledge management and IPR management to protect sensitive information.	Exclusive ownership. AEGIS intends to preserve the IPR of any breakthroughs achieved on FVT that the firm provides to the project as part of the PHOENI2X's holistic structure and continue to use them.
ATOS	The three resources CERCA, SMIR and TINTED are proprietary (closed source) owned by ATOS. SMIR, however, requires the use of TheHive platform which requires a paid license from third-party. ATOS will primarily offer their components as a service (SaaS), in a way that the solution can operate without having to grant other partners rights to use the components.	Exclusive ownership
NODALPOINT	For the SCP component, NODALPOINT may register copyright and signing NDAs when sharing SCP's details with third parties (e.g., subcontractors or collaborative partners) during or after the project's implementation.	For the SCP Key Exploitable Result, NODALPOINT intends to retain exclusive ownership of all intellectual property rights. This will ensure that NODALPOINT has full control over the SCP software, including its use, distribution, and any modifications.

3.6 Commercialisation Strategy and Roles

This section outlines the commercialisation strategy followed by the PHOENI2X consortium, based on the selected IPR protection mechanisms and ownership models agreed upon by the partners. Each partner retains full autonomy to exploit the components they have developed and own, while shared mechanisms exist to support joint opportunities.

3.6.1 Commercialisation Models

Based on the declared intentions and capabilities of each partner, the following commercialisation approaches have been identified in the following below:

Table 12 Appropriate Commercialisation Strategy per Partner

Partner	Commercialization Strategy
UPAT	Probably open source. An official decision is awaited by the University management.
SANL	SPA, ROAR, RCR and UEBA are planned to be provided as SaaS solutions, where customers will gain access through annual subscriptions. For specific capabilities, the pay-as-you-go model will be considered.
AEGIS	FVT will be provided as SaaS solution, in which customers will gain access through annual subscriptions. For specific capabilities the pay-as-you-go model will be considered.
ATOS	Exclusive or non-exclusive licenses to use the results within agreed conditions
NODALPOINT	NODALPOINT plans to establish exclusive licensing agreements for the SCP software, allowing it to manage all terms of use and distribution directly.

Taking into consideration each partner's input, the following can be suggested regarding the commercialization strategy and profit-sharing scheme:

- Each partner will employ its own policy and retain all the profits from the commercialization of the individual component/parts under its exclusive ownership.

- The PHOENI2X Service / Solution can be commercialized as a SaaS solution by a SPV.
- When a partner identifies a client and/or business opportunity, this should be provided as input to the SPV and if this becomes a project, bilateral agreements established among consortium members shall govern the way of working and the sharing of revenues and costs.
- Any disputes that may arise will be resolved through mediation and arbitration as primary mechanisms. If unresolved, legal action may be pursued in accordance with applicable laws and project agreements.
- Each partner will be responsible for maintaining and updating the components of the PHOENI2X Service / Solution that fall under its ownership.

3.6.2 Roles in Commercialisation

The following table summarises the specific commercialisation roles assumed by each partner in the context of the integrated solution.

Table 13 Role in the commercialization of the PHOENI2X Service / Solution per partner

Partner	Role in the commercialization of the PHOENI2X Service / Solution
UPAT	Academic exploitation
SANL	SANL, as a Technology Provider and Technical Coordinator, is responsible for overseeing the technical development and integration of the project's components. This includes ensuring the functionality, scalability, and security of the technical solutions. SANL will also provide continuous support during the implementation phase and ensure that all technical deliverables align with the project's objectives. Additionally, SANL will facilitate collaboration between partners by managing technical dependencies and providing guidance on the integration of individual contributions into the overarching framework. During the exploitation phase, SANL will transition into a facilitator role, supporting partners in utilizing the developed technologies effectively and identifying opportunities for further development or commercialization.
AEGIS	AEGIS will contribute to the establishment of standards for determining the rights and obligations of the PHOENI2X partners, intellectual property creators, and their sponsors with respect to inventions, discoveries, and work created, to facilitate joint exploitation of the produced framework within the scope of PHOENI2X.
ATOS	ATOS will offer their components as a service, so that they can charge subscriptions (e.g. annual) and perhaps design tiered services. In this context, their responsibility would be to keep their services running for a period after the end of the project (e.g. 6 months) to support the overall exploitation of the solution. During this period, they can provide support on best effort basis. Then, if a business opportunity arises, ATOS could be hired by the solution leader, to provide maintenance of their components, and other consulting services such as assessments for new customers.
NODALPOINT	NODALPOINT will primarily acts as an implementer, contributing technical resources and expertise in setting up large scale IT systems. NODALPOINT is also the designer and implementer of the SCP KER.

3.7 Exploitation plans per KER

3.7.1 KER #2 - ROAR

Type of Ownership:	Exclusive
Owner:	SANL
Rationale:	SANL contributed extensive expertise in cybersecurity, particularly in Security Orchestration, Automation, and Response (SOAR) solution, which is critical for the development of the ROAR tool. SANL also provided the necessary technical infrastructure and resources to design, implement, and deploy the ROAR tool, making it a foundational component of the PHOENI2X platform's objectives. As part of the project activities and in the future, SANL is and shall remain responsible for designing, developing, implementing, and maintaining the ROAR tool while ensuring it meets project objectives and partner requirements.
Expectations for the use of the tool:	The ROAR tool is expected to automate and orchestrate responses to security incidents, supporting seamless integration with external tools to improve cybersecurity incident detection, response, and management for stakeholders.
IPR Strategy and management regarding the KER:	The ROAR tool will be protected through **copyright registration** for its software and documentation, trademarks for branding, and NDAs to safeguard sensitive information. SANL will retain exclusive ownership of the ROAR tool's IP, including copyrights, trademarks, and any applicable patents. Irrespective of the role of SANL within the project, and the status of the project, ownership of the ROAR tool will remain with SANL, and knowledge transfer, documentation, and deliverable completion will ensure a smooth transition. Disputes related to the ROAR tool will be resolved through mediation and arbitration. If unresolved, legal action will be taken as per project agreements and applicable laws. SANL will be solely responsible for the ongoing maintenance, updates, and management of the ROAR tool to ensure its continued functionality and security.
Future plans regarding the market offering:	ROAR is planned to be provided as SaaS solutions, where customers will gain access through annual subscriptions. For specific capabilities, the pay-as-you-go model will be considered. As the sole IP holder, SANL will retain all profits generated from the ROAR tool, with opportunities for bilateral agreements to share royalties based on contributions.

3.7.2 KER #3 - CR

Type of Ownership:	Exclusive
Owner:	SANL
Rationale:	SANL contributes extensive expertise in cybersecurity, particularly in cyber range training and simulation. SANL also provides the technical infrastructure, resources, and platform required to design, implement,

	and deploy the Resilience Cyber Range (RCR) as a foundational component of the PHOENI2X platform. SANL is responsible for the design, development, implementation, and deployment of the RCR tool, ensuring it meets the project's objectives and provides tailored cybersecurity training and simulation capabilities.
Expectations for the use of the tool:	The RCR tool is expected to deliver advanced cybersecurity training and simulation capabilities, addressing both technical and non-technical aspects. It will support tailored exercises to enhance the resilience of systems and organizations against evolving threats.
IPR Strategy and management regarding the KER:	The CR tool will be protected through **copyright registration** for its software and documentation, trademarks for branding, and NDAs to safeguard sensitive information. SANL will retain exclusive ownership of the CR tool's IP, including copyrights, trademarks, and any applicable patents. Irrespective of the role of SANL within the project, and the status of the project, ownership of the CR tool will remain with SANL, and knowledge transfer, documentation, and deliverable completion will ensure a smooth transition. Disputes related to the CR tool will be resolved through mediation and arbitration. If unresolved, legal action will be taken as per project agreements and applicable laws. SANL will be solely responsible for the ongoing maintenance, updates, and management of the CR tool to ensure its continued functionality and security.
Future plans regarding the market offering:	CR is planned to be provided as SaaS solution, where customers will gain access through annual subscriptions. For specific capabilities, the pay-as-you-go model will be considered. As the sole IP holder, SANL will retain all profits generated from the CR tool, with opportunities for bilateral agreements to share royalties based on contributions.

3.7.3 KER #4 - TINTED

Type of Ownership:	Exclusive
Owner:	ATOS
Rationale:	ATOS has developed TINTED from scratch.
Expectations for the use of the tool:	It is expected to achieve TRL 6 by the end of the project. Therefore, we don’t really expect to pursue commercial activity right after the end of the project. Instead, we envision a period to conduct demonstrations, collect feedback and improve the features to achieve a minimum viable product. Also, it could be part of the integrated solution (KER1).
IPR Strategy and management regarding the KER:	ATOS retains full and exclusive ownership of the TINTED system.

Future plans regarding the market offering:	TINTED is planned to be provided as SaaS solutions, where customers will gain access through annual subscriptions.

3.7.4 KER #5 - CP

Type of Ownership:	Joined
Owner:	DSA, NCSA
Rationale:	DSA and NCSA are key contributors for this result, especially on the part of regulatory requirements, impact, standardisation and outreach activities. DSA and NCSA contributed to the project with expertise as National Competent Authorities entrusted with the enforcement of the NIS2 directive.
Expectations for the use of the tool:	The final PHOENI2X solution and the compliance process built upon it as tailored for critical sectors with its risk management, incident handling and reporting capabilities, can significantly assist in the compliance of the stringent requirements of the NIS2 directive.
IPR Strategy and management regarding the KER:	This KER is connected to the KER1. The operators of essential services, can adopt the PHOENI2X solution, and the national authorities can complement it with a compliance process that would allow the entities more immediate notification and assistance.
Future plans regarding the market offering:	Discussions have taken place and the possibility for DSA to sublicense the software to its Critical Infrastructure Organizations, as part of their annual administrative fees, has been in principle accepted.

3.8 Forward-Looking Strategy

The forward-looking strategy of the PHOENI2X project builds upon the foundation laid in the initial exploitation plan (D6.1) and reflects the project's commitment to ensuring long-term impact beyond its funded duration. This section elaborates on the consortium's vision for sustainable exploitation, the market outlook for key results, business and marketing considerations, and the integration of insights from technical and validation activities.

3.8.1 Market Outlook (1–3–5 years)

The market prospects for the PHOENI2X Key Exploitable Results (KERs) have been evaluated across three temporal horizons, **starting immediately after project completion**, to ensure the continuation and scaling of exploitation efforts beyond the funded period.

1-year outlook (short-term, post-project phase)

- Focus on validation and stakeholder engagement through pilot follow-ups and early deployments.
- Targeted outreach to Operators of Essential Services (OES), Managed Security Providers (MSSPs), and CERTs, leveraging the relationships established during the project.

- Preparatory actions for licensing, integration, open-source dissemination, and initial commercial engagements.

3-year outlook (medium-term)

- First wave of uptake and adoption expected for components with high Technology Readiness Levels (TRL) and demonstrated pilot performance.
- Establishment of strategic partnerships enabling sector-specific deployments (e.g., healthcare, energy).
- Continued refinement and scaling of business models adapted to the market dynamics of each KER.

5-year outlook (long-term)

- Full commercialisation or institutional integration of mature KERs into operational environments.
- Potential bundling of multiple KERs into comprehensive cybersecurity and resilience offerings.
- Contribution to strengthening national and EU-level cybersecurity capabilities and strategic frameworks through partnerships, standardisation, and policy influence.
- Adoption of the solution as part of the service offerings of National Cybersecurity Authorities.

3.8.2 Business and Marketing Strategy

Each KER follows an individualised path to exploitation, supported by a shared strategy to increase visibility and market readiness:

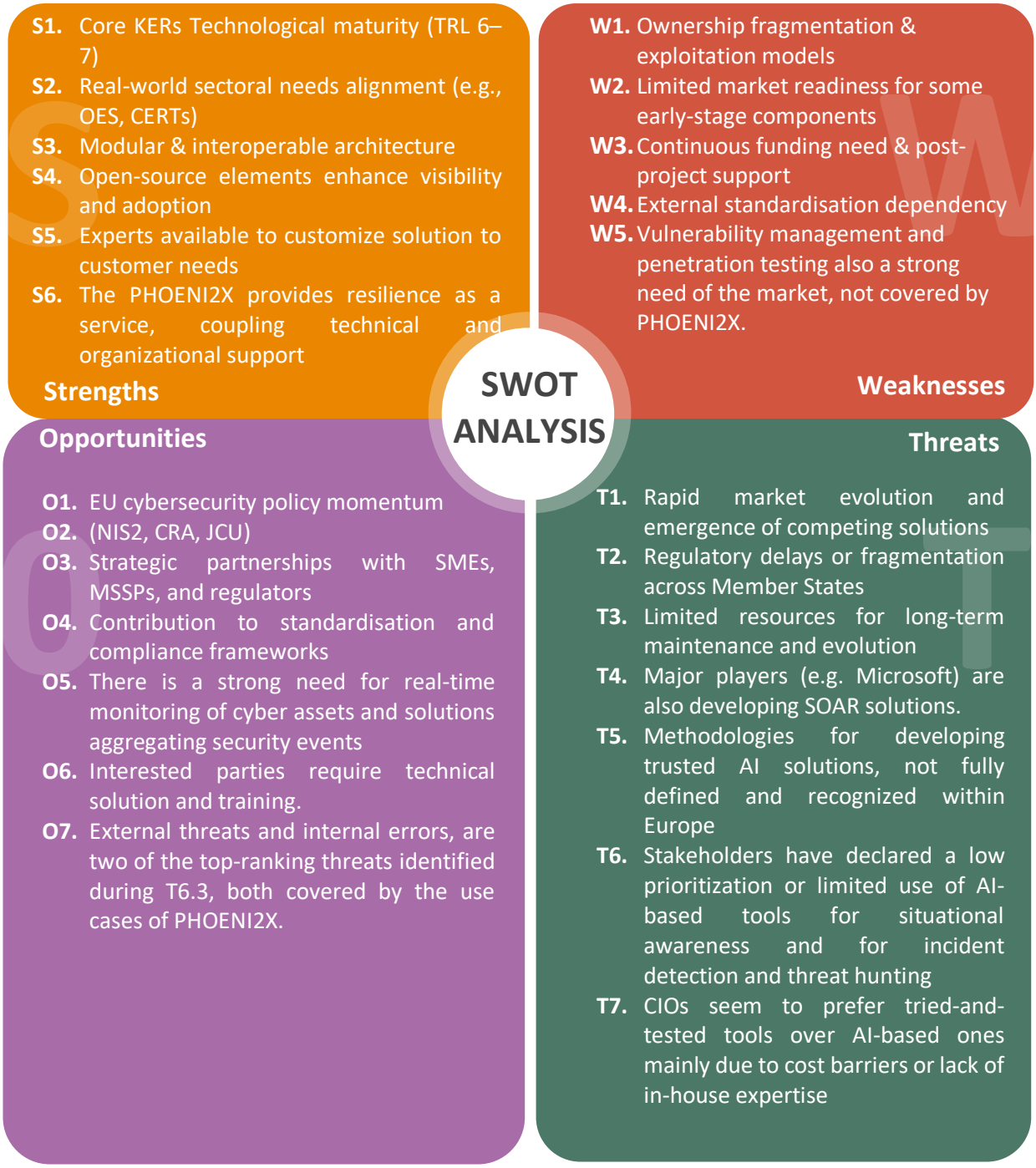
- **SANL** aims to license its SPA/ROAR/RCR/UEBA components to MSSPs and cybersecurity integrators.
- **AEGIS** will retain exclusive rights to the Forensics Visualisation Toolkit (FVT), positioning it for adoption by CERTs and law enforcement agencies through direct engagement.
- **ATOS** plans to integrate CERCA/SMIR/TINTED into its managed security services portfolio, offering them as part of a holistic cyber resilience suite.
- **NODALPOINT** intends to productise and commercialise the SCP solution, targeting health and public sector clients.
- **UPAT** will maintain its IDS as an open-access tool for academic and research communities, promoting collaboration and continued development.

On a consortium level, the project is pursuing a combined value proposition through:

- Thematic bundling of interoperable KERs.
- A shared visual identity and messaging strategy to unify communication.
- Participation in targeted industry events and standardisation fora.

To support strategic exploitation planning, the consortium has conducted a business model canvas of the PHOENI2X Key Exploitable Results (KERs). This analysis, during the second reporting period was combined with the results of the validation analysis (T5.4) and the results of the stakeholder engagement and liaison activities (T6.3) and a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis was carried out. The results of the SWOT analysis are depicted in Figure 31. S5, S6, O5, O6, O7, W5. T4, T5, T6 and T7 are directly connected with the results of tasks 5.4 and 6.3.

Figure 31: KERs SWOT Analysis



3.8.3 Sustainability and Funding Pathways

Sustainability beyond the project lifetime is a key objective. The following mechanisms are being pursued:

- **Inclusion in EU innovation clusters** (e.g., ECSO, AIOTI) to maintain visibility and collaboration.
- **Follow-up project proposals** under Horizon Europe or Digital Europe programmes for further development and scaling.
- **Internal institutional uptake** for partners such as ATOS and SANL, embedding results in their service portfolios.

- **Open-source communities** for continuous improvement of selected KERs (e.g., UPAT's IDS).
- **Embedding in Standards** for the establishment of an international recognized baseline for the related playbooks and the shared communication taxonomy in case of incidents.
- **Public-private partnerships** (PPP) to scale pilot implementations.

In alignment with the project's open science and innovation principles, PHOENI2X commits to maximising the availability and reusability of its technical outcomes. Where feasible, selected components including the platform, models, and associated outputs will be released under open-source licenses (e.g., Apache 2.0, MIT, or Creative Commons). This approach enhances transparency, fosters adoption across stakeholder communities, and supports sustainability beyond the project lifetime.

With the project entering its final phase, concrete commitments have been established among partners to maintain key KERs, pursue open-source dissemination, and seek continuation via EU innovation networks and institutional uptake.

3.9 Post-Project Business Plan and Marketing Strategy

The post-project business plan and marketing strategy aim to ensure the long-term sustainability and uptake of PHOENI2X results across commercial, institutional, and open-source ecosystems. Each KER is supported by an exploitation path tailored to its ownership, technology maturity, and market readiness, with specific business models and dissemination channels identified during Task 6.2.

3.9.1 Draft Post-Project Business Plan

3.9.1.1 Adopted Business Models

Table 14, depicts the business models, that have been identified as more fitting for each of the KERs of the project.

Table 14 Business Models per KER

KER	Business Model	Ownership
PHOENI2X Solution	Bundled service solution offered to public and private sector organisations (OES, MSSPs). Modular licensing model based on deployment needs. More details are provided within Section 3.4.	UPAT, SANL, AEGIS, ATOS, NODALPOINT
ROAR Incident Response Tool	Commercial licensing to Managed Security Providers and cybersecurity consulting firms. Potential SaaS (Software as a Service) deployment.	SANL
CR Cyber Range Tool	On-premise deployment for critical infrastructure operators and cybersecurity training providers. Consulting and setup services.	SANL
TINTED CTI Analytics Platform	Integration into MSSP service portfolios or licensing to SOC operators. Customisation services for sectoral needs.	ATOS
CP Compliance Process	Institutional uptake by national regulatory bodies; consultancy-based delivery	DSA, NCSA

3.9.1.2 Partners' Roles

Exploitation of PHOENI2X results follows a decentralised approach based on ownership and technological contribution. Roles are allocated as follows:

- SANL: Owner and exploiter of ROAR and CR; responsible for commercial licensing, packaging, and post-project technical support.
- ATOS: Owner and exploiter of TINTED; plans integration into MSSP offerings; responsible for business development in enterprise markets.
- UPAT: Contributor to the PHOENI2X integrated solution; responsible for maintaining and disseminating the open-source IDS component.
- NODALPOINT: Owner of SCP; will explore bundling with other KERs; focus on institutional and critical sector integration.
- AEGIS: Owner of FVT; plans vertical market partnerships and sectoral licensing.
- DSA & NCSA: Institutional exploitation of CP with potential support for national rollouts.

For the integrated PHOENI2X Solution (KER_01), joint branding and bundling efforts are envisaged. Partners will contribute based on their owned components, with shared outreach and potential cross-licensing under discussion.

3.9.1.3 Revenue Models

Per case, the following revenue models have been identified:

- **License fees** for proprietary tools (e.g., ROAR, CR, TINTED)**.**
- **Subscription-based models** for managed deployments (e.g., SaaS variants).
- **Consulting services** for adaptation, training, and deployment (especially for CP and the integrated solution).
- **Open-source dissemination** to build community engagement and policy relevance (e.g., UPAT components).

It should be noted that the variation of the KERs and the nature of the PHOENI2X (as an integrated solution with different components), is also inherited in the revenue models identified.

3.9.1.4 Cost and Investment Considerations

While core component development was completed during the project, the transition to market-ready offerings requires further investment. Key cost categories include:

- Packaging and productization of individual tools and components,
- Long-term maintenance of open-source elements,
- Legal services and IP agreements (e.g., for joint ownership management),
- Marketing, outreach, and stakeholder onboarding.

These represent strategic post-project investments necessary to operationalise and scale exploitation activities.

3.9.1.5 Funding Opportunities Post-Project

To address the above cost needs and support scale-up efforts, the consortium will explore the following funding mechanisms:

- Participation in EU programmes (e.g., Digital Europe, Horizon Europe Innovation Actions),

- Access to national cybersecurity or digital transformation grants,
- Strategic partnerships with private sector actors (e.g., integrators, vendors),
- Engagement in EU-level cybersecurity initiatives (e.g., ECSO clusters) for co-investment and **joint projects**.

3.9.2 Marketing Strategy

This section provides some further information of a preliminary marketing strategy to be activated after the end of the project, in order to achieve the post-project sustainability and exploitation goals. As also identified in D6.1. the PHOENI2X project has a variety of identified stakeholders. Each of these stakeholders have different needs and expectations in relation to the PHOENI2X Service / Solution. The main target markets and stakeholders, as well as the value propositions for each KER are presented in the sections below.

3.9.2.1 Target Markets and Stakeholders

Table 15, depicts the types of stakeholders identified, that have an interest and could be targeted as part of the post-project exploitation and sustainability activities of the project. These stakeholders are a subset of the list of Stakeholders identified and depicted in D6.1. following an extensive Stakeholder analysis process.

Table 15 Stakeholders and their interests

Type of Stakeholder	Interest
Critical infrastructure organizations (CIOs) (e.g. in energy, transportation, health domains) or in general, organizations with obligations stemming from regulatory frameworks such as GDPR, NIS2, eIDAS.	Potential customers / users of the PHOENI2X Service / Solution
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.	Potential customers / users of the PHOENI2X Service / Solution
(Managed) 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	Potential customers / users of the PHOENI2X Service / Solution Potential resellers of the solution to their customers or as part of a managed security service
Public Sector and Institutional Users especially for CP and the compliance suite	Indirectly interested in the PHOENI2X Service / Solution. Direct interest in adoption of the CR component.
Policy makers at any level (Ministries and Governments, other related European and national agencies, Standard Developing Organizations, etc.)	Interested in adopting the best practices related to incident response and business continuity play-books as well as the relevant communication taxonomy.
Academia and Research	Interested in gaining insights and building on top of the provided solutions.

3.9.2.2 Value Propositions per KER

Table 16, depicts core values identified for each KER following an analysis facilitated on the CANVA model. These core values will be the main point used within the marketing and communication activities after the end of the project.

Table 16 Core Value per KER

KER	Core Value
PHOENI2X Solution	End-to-end cyber resilience suite combining detection, response, compliance, and secure communication
ROAR Incident Response Tool	Streamlined incident response with real-time orchestration
CR Cyber Range Tool	Interactive cyber range tailored to critical infrastructure and training
TINTED CTI Analytics Platform	Advanced threat hunting and CTI analysis
CP Compliance Process	Structured approach to cybersecurity compliance (aligned with NIS2, Resilience Act)

3.9.2.3 Communication & Outreach Channels

Table 17 and Table 15, depicts the communication and outreach channels used per type of stakeholder as identified in Table 15. For each case of stakeholder, the interest is different and the same applies to the channels suitable for communication and outreach.

Table 17 Communication and Outreach Channels per type of stakeholder

Type of Stakeholder	Communication and Outreach Channels
Critical infrastructure organizations (CIOs) (e.g. in energy, transportation, health domains) or in general, organizations with obligations stemming from regulatory frameworks such as GDPR, NIS2, eIDAS.	Participation in industry events (e.g., ENISA Cybersecurity Conference, ECSO WG meetings). Publication of white papers and success stories from project pilots. Stakeholder-targeted webinars and hands-on demonstrations
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.	Participation in industry events (e.g., ENISA Cybersecurity Conference, ECSO WG meetings). Publication of white papers and success stories from project pilots. Stakeholder-targeted webinars and hands-on demonstrations
(Managed) 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	Participation in joined activities with other EU funded R&D projects. Participation in new EU funded R&D projects. Participation in industry events (e.g., ENISA Cybersecurity Conference, ECSO WG meetings). Publication of white papers and success stories from project pilots.

Type of Stakeholder	Communication and Outreach Channels
Public Sector and Institutional Users especially for CP and the compliance suite	Participation in joined activities with the National Cybersecurity Authorities. Publication of white papers and success stories from project pilots, highlighting the advantages afforded to the national authorities from the adoption of the solution.
Policy makers at any level (Ministries and Governments, other related European and national agencies, Standard Developing Organizations, etc.)	Policy briefings and alignment with NIS2 and Cyber Resilience Act developments Participation in standardisation efforts (e.g., ETSI, CEN-CENELEC, ISO, OASIS)
Academia and Research	Publication of scientific publications. Participation in scientific conferences.

3.9.2.4 KPI Monitoring (1–3–5 Years)

Table 18 and Table 15, depicts some of the initial KPIs that have been collectively set by the project split into periods following the project end. These KPIs are preliminary and are subject to the decisions and the developments to individual components by the project partners.

Table 18 KPIs to be monitored after the end of the project

Timeframe	Target
1 year	Launch of 2–3 licensing pilots, integration in 1 OES
3 years	Commercial offering by SANL, ATOS, NODALPOINT In the case of the PHOENI2X solution, new joint exploitation packages shall be defined, drawing from the practical implementation of projects.
5 years	Institutional uptake of the CP by another two authorities. Publication of part of the feedback of the project in standards.

3.10 Summary and Exploitation Roadmap

This deliverable presents the structured and systematic approach followed by the PHOENI2X consortium to identify, assess, and plan for the exploitation of its Key Exploitable Results (KERs). As the project enters its final phase, the consortium has focused on consolidating efforts, validating partner intentions, and preparing the ground for sustainable uptake of its technological innovations beyond the project duration.

Through dedicated methodologies, iterative refinement, and collaborative engagement across work packages, the consortium has achieved the following:

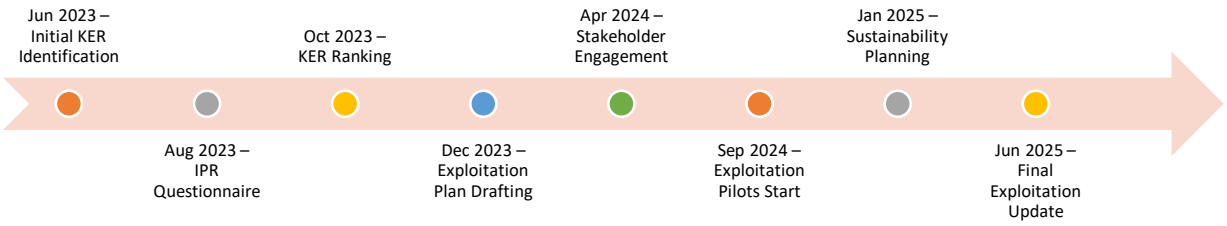
- Identified and clearly characterised a set of core Key Exploitable Results (KERs), mapped to specific technical outcomes and aligned with sectoral needs (e.g., OES, CERTs, MSSPs).
- Collected structured input via targeted questionnaires and consortium-wide consultations, resulting in validated IPR ownership, intended protection mechanisms, and envisioned exploitation modes for each KER.
- Evaluated the technological maturity level (TRL), innovation level, and market potential of the results, prioritising high-impact assets for early exploitation.

- Developed both individual exploitation strategies — reflecting each partner's strengths and business orientation — and joint approaches leveraging synergies across joined KERs.
- Identified potential risks and constraints to exploitation (e.g., legal, market, technical), and designed appropriate mitigation strategies supported by stakeholder mapping and targeted engagement plans.
- Refined partner-specific business models, licensing scenarios, and revenue channels.
- Implementation draft exploitation pilots and demonstration activities involving end-users and domain stakeholders.
- Establishment of sustainability pathways including open-source dissemination, integration into commercial offerings, institutional uptake, and clustering with EU initiatives.
- Alignment with evolving EU cybersecurity policy developments (e.g., NIS2, Cyber Resilience Act), and contribution to standardisation and regulatory discussions via strategic positioning of KERs.

To support this vision, a structured mapping of key stakeholder groups and corresponding exploitation channels has been developed.

Finally, the roadmap in Figure 32 below outlines the main exploitation milestones across the PHOENI2X implementation timeline. It serves as a reference for aligning activities, monitoring progress, and ensuring timely delivery of key exploitation objectives.

Figure 32: Exploitation Milestones Timeline



This visual plan ensures clarity on timing, responsibilities, and expected outcomes, and reinforces the consortium's long-term commitment to maximising the reach and sustainability of its innovations.

The exploitation roadmap established through this task will serve as a bridge between project outcomes and their long-term real-world impact, ensuring that PHOENI2X innovations continue to evolve, scale, and support Europe's cyber resilience goals beyond the scope of the project itself.

As the project approaches its final reporting phase, PHOENI2X partners are already activating post-project sustainability pathways, ensuring that key results are not only protected but also ready for continued uptake and real-world deployment

4 STANDARDIZATION

4.1 PHOENI2X standardization strategy

Deliverable D6.1 produced by the PHOENI2X project on month 18, provided an overview of the concept, terms and actors related to Standardization. From the beginning of the project, a standardization strategy was devised split into the following steps:

1) Identification of key topics of the PHOENI2X project;
2) Identification of possible standards that can be of use to the project and
3) Identification of possible standardization efforts where the project could provide useful contribution.

Within this strategy, standards were considered in multiple ways, e.g., as incoming knowledge, as a basis to be adopted and built upon and as means for the valorisation of the project results.

Various SDOs (Standard Developing Organizations) were identified and already by month 18, the project could claim the usage of standards like: ETSI TR 103 331, ETSI TR 103 303, ISO/IEC 27031, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3, ISO 22301, ISO 22317, CACAO Security Playbooks, STIX OASIS Standard, TAXII OASIS Standard, STIX v2.1 Interoperability Test Document and others.

4.2 Contribution to Standards

In terms of standards development, the PHOENI2X project, participated in the following:

4.2.1 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 participating in relevant meetings and providing feedback on the relevant requests and assignments.

4.2.2 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[30].

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

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[31]:

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

- 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.

Currently, three projects are under development within CEN/CLC/JTC 13/WG 9:

[30] https://www.din.de/en/getting-involved/standards-committees/nia/european-committees
[31] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

a) prEN XXX (WI=JT013089). Cybersecurity requirements for products with digital elements - Principles for cyber resilience.

b) prEN XXX (WI=JT013091). Cybersecurity requirements for products with digital elements – Generic Security Requirements.

c) prEN XXX (WI=JT013090). Cybersecurity requirements for products with digital elements – Vulnerability Handling.

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.

4.2.3 OASIS

In alignment with its strategic goal to foster interoperability, sustainability, and consistency with broader European cybersecurity initiatives, PHOENI2X has remained actively involved with prominent international standardization bodies and community-led efforts. The project acknowledges that adopting and contributing to open standards is essential for enabling seamless information exchange, automating response mechanisms, and ensuring compatibility with current and future cybersecurity infrastructures. Throughout this reporting period, PHOENI2X has prioritized harmonizing its technical progress with developments in standards such as CACAO, STIX/TAXII, and TAC. Engagements have also extended to collaborative spaces including the Open Cybersecurity Alliance (OCA). This section provides an overview of PHOENI2X's activities in the standardization landscape and illustrates how these efforts have influenced the technical architecture and implementation of the PHOENI2X platform.

4.2.3.1 OASIS CACAO TC

The Collaborative Automated Course of Action Operations Technical Committee (CACAO TC)[32] focuses on defining a standardized playbook schema and taxonomy for describing cybersecurity response workflows. These orchestration workflows, encoded in a machine-readable format, enable organizations to exchange playbooks easily across teams and organizational boundaries.

PHOENI2X has deepened its involvement in this area by actively contributing to the CACAO TC's ongoing standardization efforts. The CACAO specification has been adopted as a foundational element within PHOENI2X, underpinning both internal automation logic and inter-organizational coordination. A key driver of these contributions has been the University of Oslo (UiO), a project partner that serves as both co-chair and secretary of the CACAO technical committee.

Drawing from PHOENI2X use cases and pilot implementations, valuable feedback has been channeled into the CACAO TC's work. One notable outcome of this collaboration is the development of the CACAO Layout Extension[33], authored by PHOENI2X and accepted by the CACAO Technical Committee as an official part of the standard. This extension, now integrated into CACAO version 3, defines a consistent approach to visually representing CACAO playbooks, improving usability and ensuring uniform rendering across tools and implementations.

[32] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=b75cccb8-adc6-4de5-8b99-018dc7d322b6

[33] https://docs.google.com/document/d/1h0uAHJ8rfIp98MZdGivZp0UXb12SE_FaXA8X3-KKvMk/edit?tab=t.0

The forthcoming version of CACAO, shaped in part by these contributions, is designed to enhance the specification's robustness and maturity—positioning CACAO as a reliable and future-proof standard for cybersecurity playbooks across diverse operational environments.

4.2.3.2 OASIS CTI TC

The Cyber Threat Intelligence Technical Committee (CTI TC)[34] under OASIS is responsible for developing the STIX and TAXII standards, which provide a structured and interoperable framework for representing and exchanging cyber threat intelligence across organizational boundaries.

PHOENI2X has incorporated these standards to support the structured sharing and automated processing of threat intelligence within its platform. In selected operational scenarios, the project has explored the development of STIX extensions to better accommodate specific threat models and domain requirements.

A key contribution in this context is the creation of the STIX 2.1 Course of Action (COA) Playbook Extension[35], developed by PHOENI2X in collaboration with the Open Cybersecurity Alliance. This extension introduces structured support for playbook-related metadata directly within STIX COA objects, bridging the gap between threat intelligence and cybersecurity automation. By aligning the STIX data model with CACAO playbooks, the extension enables tighter integration between intelligence-driven insights and actionable response workflows. The specification has been published as part of the official OCA STIX Extensions repository[36], further promoting reuse and standardization across the cybersecurity community.

4.2.3.3 OASIS TAC TC

The Threat Actor Context Technical Committee (TAC TC)[37] is developing a formal ontology to provide a semantic framework for representing cyber threat intelligence (CTI), extending the STIX 2.1 standard using OWL (Web Ontology Language). This enables more expressive modeling, improved interoperability, and support for advanced reasoning and analytics.

PHOENI2X, through its consortium partner UiO, has made a significant contribution to the TAC TC's standardization efforts by authoring and maintaining the TAC Ontology. This ontology formalizes the STIX 2.1 specification into a modular, semantic structure that allows complex relationships to be represented beyond the limitations of the original JSON format. Its modular design—where each STIX Domain Object is represented in a separate OWL module—promotes extensibility, reuse, and integration with domain-specific ontologies, such as those covering assets, vulnerabilities, or threat actor libraries.

The TAC Ontology is published and maintained as an open standard through OASIS and is openly available via GitHub[38], forming a cornerstone for interoperable, semantically rich CTI modeling. It

[34] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=c6c33da0-d1ee-42dd-9427-018dc7d32277
[35] https://github.com/opencybersecurityalliance/stix-extensions/blob/main/contexts/playbook/STIX2.1_COA_Playbook_Extension_v4.asciidoc
[36] https://github.com/opencybersecurityalliance/stix-extensions
[37] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=33f0d182-232a-4c56-aba6-018dc7d3f415
[38] https://github.com/oasis-open/tac-ontology/tree/develop

supports integration with external knowledge models, enabling organizations to unify heterogeneous sources of threat intelligence under a shared semantic framework.

To further demonstrate the applicability of the ontology, PHOENI2X has developed a proof-of-concept implementation, described in Deliverable D3.2, section 4.4.2, showcasing the use of AI to extract structured CTI from unstructured text sources using the TAC Ontology as the target schema. This implementation exemplifies how formal standardization work can be operationalized to enable advanced, ontology-driven CTI processing, enhancing automation and analytical capabilities.

4.2.3.4 CACAO Ontology

As part of its effort to advance the state-of-the-art in cybersecurity automation, PHOENI2X has initiated and led the effort of creating the CACAO Ontology—a semantic extension of the OASIS CACAO playbook framework (as described in D3.2 in section 4.5). Recognizing the limitations of JSON-based data structures in modeling complex relationships and enabling advanced analytics, the ontology provides a formal OWL-based representation of CACAO playbooks. This enables reasoning, inference, and semantic classification of playbooks, allowing for deeper integration with other cybersecurity models and data sources. The ontology supports a more expressive and machine-interpretable understanding of playbook components, such as investigation types, tool integrations, and operational procedures.

By aligning with the principles of the Semantic Web, PHOENI2X positions CACAO playbooks as knowledge graph instances that can be queried, linked, and reasoned over—enhancing automation, interoperability, and situational awareness across cybersecurity systems. The CACAO Ontology introduces a modular and extensible structure that mirrors the CACAO specification while transitioning toward a standards-based serialization format such as JSON-LD and RDF. This approach ensures backward compatibility while opening new opportunities for intelligent orchestration and system integration. The ontology is planned for open-source release, with the goal of ongoing community-driven maintenance and confirmed adoption as an official component of the CACAO standard under OASIS.

4.3 Other standards related activities

PHOENI2X project, along with projects CYBERSECDOME[39] and SYNAPSE[40] jointly applied for the open call of the HSBooster[41] consultancy service. The HSBooster consultancy Service focuses on providing expert consultancy on various standardisation-related aspects of a given research project. The consultancy aims to enhance the project's understanding and engagement with standardisation processes to achieve effective results.

The projects discussed and jointly decided, also due to their different timelines and activities related to standards to request a dedicated standards-mapping webinar, where the HSBooster expert would provide information on standardization and specific feedback on the standardization activities and strategy of the projects.

The webinar took place on the 20th of March 2025 and the agenda of the meeting is depicted in Figure 33. Due to the restricted nature of the PHOENI2X project and the project specific information exchanged during the webinar, the webinar was only accessible to partners of the involved projects.

[39] https://cybersecdome.eu/
[40] https://www.synapse-project.eu/
[41] https://www.hsbooster.eu/

The PHOENI2X project was represented by Ms. Argyro Chatzopoulou (APS) and the strategy, results and recommendations of the PHOENI2X project on standardization were presented. Figure 34 and Figure 35 are screenshots of the presentations from the HSBooster expert Mr. Henrich Pöhls and Ms. Argyro Chatzopoulou (APS).

During the webinar, further recommendations were provided by Mr. Pöhls on how standardization could be effectively integrated and supported within a European Funded project:

- Embed standardization as early as possible within the project (if possible from the proposal).
- Provision of standards related training early on, through suitable experts.
- Creation of a standardization strategy early on.
- Identification of tasks that would incorporate standards.
- Allocate appropriate time for these tasks, since standardization takes time.
- Identify the standards of interest and the SDOs, as early as possible.
- Use standards as much as possible.
- Select and build upon standards of interest.
- Be flexible, the timelines of standards are not aligned to the project's timeline.
- Identify the partners and people that will be participating / reaching out to the SDOs.
- Keep evidence of standardization contribution (not only the feedback text but also travelling and participation in relevant meetings is included in the standardization work also).
- Standardization takes time and effort, so this has to be budgeted, allocated and in line with the project's timeline (instead of the standards' timelines).
- Standardization is a tool that can be used for the valorization of knowledge.

Invitation to a joint workshop on

Insights & lessons learned in standardisation of incident response

by PHONI2X, CYBERSECDOME, SYNAPSE and Hsbooster Expert Dr. Pöhls

on 20th of March 10-13 C.E.T. via ZOOM

Agenda

1 – 15 min. – Welcome and introduction of participants – All participants
2 – 30 min. – Standardisation in General – Henrich C. Pöhls (HSBooster expert)
3 – 30 min. – Lessons learned and experiences by PHOENI2X – Expert(s) from PHOENI2X project
4 – 15 min. – Current approach from CYBERSECDOME – Expert(s) from CYBERSECDOME project
5 – 15 min. – Current approach from SYNAPSE – Expert(s) from SYNAPSE project
6 – 30 min. – Feedback from HSBooster expert and discussion – All participants
7 – 30 min. – Suggestions for Future Steps – Henrich C. Pöhls (HSBooster expert)
8 – 16 min. – Discussion and Closing remarks – All participants

Duration 3h no breaks

Delivery virtual, via ZOOM http://zoom.poehls.com

Figure 33: HSBooster webinar Agenda

Figure 34: Insights by the HSBooster expert on the standardization process

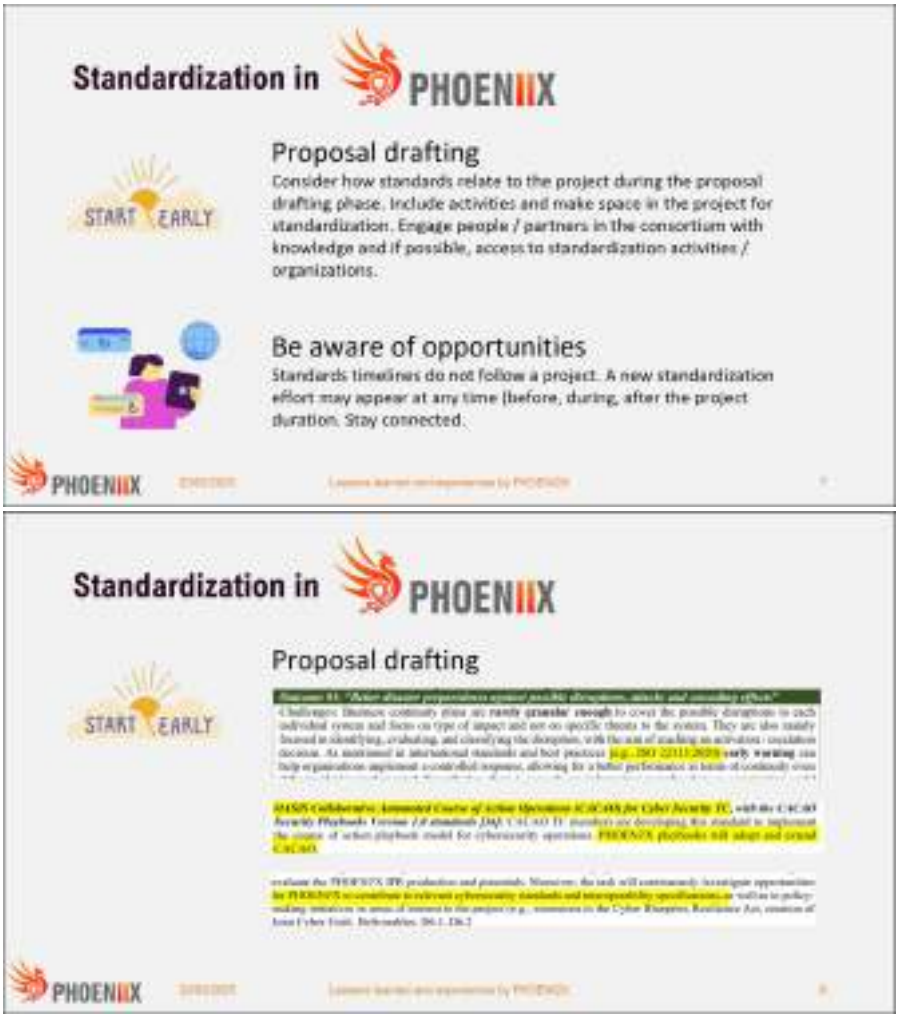


Figure 35: Screenshots from the PHOENI2X project standardization presentation

4.3.1 FIRST CTI SIG and FIRST Automation SIG

The Cyber Threat Intelligence[42] (CTI) Special Interest Group of FIRST focuses on advancing the practical application of threat intelligence capabilities and fostering discussions around CTI standards. This group is particularly relevant to the modeling, representation, and exchange of cyber threat intelligence across organizations.

The Automation[43] Special Interest Group within FIRST aims to equip members with best practices for incident response automation and to track developments in cybersecurity orchestration and automated defense mechanisms. Its work is closely aligned with ongoing advancements in cybersecurity automation.

PHOENI2X has actively engaged with both the CTI and Automation Special Interest Groups at FIRST. Participation in these forums has offered valuable insight into current best practices, operational challenges, and emerging trends in the fields of threat intelligence and automation. These learnings have been directly incorporated into the project's technical roadmap and system design. Additionally,

[42] https://www.first.org/global/sigs/cti/
[43] https://www.first.org/global/sigs/automation/

PHOENI2X has contributed by sharing updates on its use of open cybersecurity standards and its alignment with community-driven best practices.

4.4 Contribution to Policy initiatives

The PHOENI2X project, is aligned to requirements of organizations regarding incident response and business continuity preparedness and communication as prescribed in regulatory documents like NIS2 Directive. During the lifetime of the project, the project partners noted of any opportunities were feedback – related to the main topics of the project – to policy makers could be provided. This monitoring resulted in the contribution of the project to the following:

4.4.1 ENISA technical guidance for the cybersecurity measures of the NIS2 Implementing Act

ENISA is developing technical guidance to support EU Member States and entities with the implementation of the technical and methodological requirements of the NIS2 cybersecurity risk-management measures outlined in the Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024.

ENISA develops this technical guidance to provide:

- Additional advice and tips on what to consider when implementing a requirement and further explanation about concepts and terms used in the legal text;
- Examples of evidence, which could be used to asses if a requirement has been met;
- Tables, mapping the security requirements in the Implementing Regulation to European and international standards, as well as national frameworks.

As part of this implementation activities, ENISA provided a draft of the technical guidance for industry consultation through the Have your say function of the European Commission. The consultation was open until the 9th of January 2025, and the PHOENI2X project provided feedback in the form of a document and the required xls feedback form (through an email as prescribed). Since the PHOENI2X project, focuses specifically on the subject of Incident Handling and Response and Business Continuity the feedback was focused on these two parts.

In the following two sections, the feedback of the PHOENI2X project is provided.

4.4.1.1 Incident handling

The guidance provided, connects different subjects and phases related to incident handling and response. It provides information and guidance from the activities of logging and monitoring, to security event and security incident management.

Throughout the guidance, it is recommended that incident handling and response should be aligned with

- the objectives related to business continuity and disaster recovery,
- the results of the risk assessment,
- legal requirements/obligations and
- relevant best practices.

However, the guidance does not provide a systematic way that entities could implement the above and achieve this alignment by default.

Specifically, we recommend the following to be added:

[Guidance text of 3.1.2.] As indicated in 4.1.3. the relevant entity shall carry out a business impact analysis to assess the potential impact of severe disruptions to their business operations and shall, based on the results of the business impact analysis, establish continuity requirements for the network and information systems. In practice, this activity shall provide the organization with the measurable RTOs, RPOs, SDOs and MAO (Maximum Acceptable Outage) per business process.

The incident handling policy and related documentation, should take them in consideration and should clearly identify the series of activities that need to be implemented as part of the incident response in order to achieve the business continuity objectives of the organization.

To ensure that the activities are carried out as needed and that the flow of activities is effectively and efficiently implemented, standardized practices and tools like playbooks should be used. Such playbooks should be designed and implemented, encoding the relevant incident handling processes, incorporating flows both for activities that relate to incident response as well as those that are related to business continuity and disaster recovery.

Standardized tools and processes such as playbooks can support organization in the categorization of incidents, so that the necessary information is included from the beginning in a way that decision making can be effectively supported.

By designing and having such standardized processes the organizations can include crucial elements of the incident response process (e.g., roles, actions, tools, thresholds) and have them ready and automated (to the degree possible) in case of an incident, making the entire process more practicable and effective.

Examples of relevant evidence could include the specific procedures for incident response, the identification and assignment of roles, the evidence that the standardized methods and tools e.g., playbooks are specified, as well as evidence that a relevant system and/or mechanisms are in place to execute said methods and playbooks.

[Guidance text of 3.1.3.] The policy and the related incident management documentation should identify the necessary roles. Such roles, could be named as the entity needs (based on its organizational structure), and should incorporate at least the following tasks:

- coordination and management of event notifications and alerts that are raised either by information systems or individuals,
- evaluation of the event and declaration that an incident occurs / has taken place,
- activation of the IRT(s) and coordination of its/their activities,
- recording of all information on the incident and its resolution,
- completion and dispatching the incident report, with their proposals for improvement,

- coordination with internal and external organisations following the incident management team direction with respect of incident handling - carry out the assessment based on predefined criteria laid down in advance, and on a triage to determine prioritisation of incident containment and eradication,
- assess the existence of recurring incidents as referred to in Article 4 of this Regulation on a quarterly basis,
- review the appropriate logs for the purposes of event assessment and classification,
- review incidents related to ICT products and ICT services from suppliers and service providers,
- ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures,
- test the incident response provisions and plans – including communication paths, responsibilities and decision making,
- test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks,
- implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures,
- perform incident containment, to prevent the consequences of the incident from spreading,
- perform eradication, to prevent the incident from continuing or reappearing,
- recover from the incident, where necessary.

For each one of these tasks, the entity should identify the necessary skills and knowledge that the personnel / parties assigned with these tasks, shall have, in order to implement them effectively.

The entities can use already established skills frameworks e.g. the ECSF to assist them in identifying the necessary skills and knowledge.

The entities should ensure that these assigned persons are competent on the basis of appropriate education, training, or experience and where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken. For the existence of the necessary competence, the entities should retain appropriate documented information as evidence of competence.

Further, as noted for 3.1.2 above, the procedures being tested & reviewed should also consider their encodings in the relevant playbooks, leveraging these playbooks to guide the training (e.g., incorporating them in the relevant exercises), and eventually using the feedback from this testing & review to update the playbooks (e.g., to encode more efficient or more effective procedures). The tracking of playbook updates (version history) could be an example of relevant evidence, in this context.

[Guidance text of 3.5.2.] As previously noted, the documented Incident Response procedures mentioned in this paragraph could leverage the use of playbooks, as these will not only provide a structured, tracked and shareable means of encoding these procedures, but also pave the way for automating the execution of these procedures (allowing for more efficient & timely response; see goal of paragraph 3.5.1.). Relevant standards should be considered for encoding these playbooks, such as the OASIS Collaborative Automated Course of Action Operations (CACAO) Security Playbooks Version Specification (now at V2.0; https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html). Relevant evidence would include the specified playbooks themselves, as well as statistics, logs & relevant metrics from their execution (these logs would also be relevant for previous paragraphs, such as 3.2.2 & 3.2.7, which refer to the needs of logging, and the associated provided guidance).

[Guidance text of 3.5.4.] Per previous recommendations, if playbooks are considered in the implementing guidance, this paragraph and other relevant parts of the guidance, should be updated to reflect the need to log incident response information generated from playbook execution.

[Guidance text of 3.5.5.] To include testing (and eventual updates) to the relevant playbooks, as previously noted.

4.4.1.2 Business Continuity and Crisis Management

The proposed guidance, is in line to a large degree with relevant international best practices and standards.

But, in order to further support the implementation of the business continuity plans and the identification of the recovery priorities, further guidance could be added.

Specifically, we recommend the following to be added:

[Guidance text of 4.1.2.] As recommended in 3.1.2., there should be a clear connection and alignment between business continuity objectives and incident response. As such, in the contents of the business continuity plan, a reference or a description / connection should be made with the incident handling policy, plan and procedures.

[Guidance text of 4.1.3.] MAO (Maximum Acceptable Outage) should be added on the outputs of the Business Impact Analysis process, as indicated by relevant international standards [ISO 22300:2021].

The relationship between the business continuity plan, the disaster recovery plan and the crisis management plan should be included in the guidance as well as their definitions, since there are multiple resources providing varying definitions.

[Guidance text of 4.1.4.] As in the case of incident handling testing, the different methodologies that could be used for the testing and review of the business continuity and disaster recovery plans, should be added. Especially since the entities affected by this guidance, have very high

availability requirements (always on), specific guidance should be provided regarding how testing of continuity and disaster recovery provisions could be implemented. Especially, the guidance should indicate that all provisions should be tested at least through the use of one methodology, at least once a year.

Different methodologies which could be utilized could be:

- alternative locations for personnel,

- disaster recovery locations – hot sites,

- digital twins,

- simulations,

- table top exercises and others.

Finally, for the effectiveness of the different types of the testing methodologies, the use of only table top exercises should be limited and should not be used in repeated tests of the same provision.

4.4.2 ENISA pilot activities for the Cyber Incident Emergency respondent profile

As part of the requirements of the Communication on the Cybersecurity Skills Academy[44], ENISA has been tasked with the creation of an attestation scheme for cybersecurity skills. Specifically, the communication mentions that:

"It is also necessary to provide assurances to professionals that the trainings they undertake are of the required quality. In this regard, ENISA will develop a pilot project, exploring the setup of a European attestation scheme for cybersecurity skills."

ENISA has started an internal project and the pilots of an attestation of scheme for the Incident Emergency response profile.

The 'Cyber Incident Emergency respondent' role, is a specialized subset of the broader ECSF[45] (European Cybersecurity Skills Framework) incident response role which has been tailored to support the EU Cybersecurity Reserve mentioned in the Cyber Solidarity Act[46]. The role includes specific tasks, skills, and knowledge requirements, with defined minimum skills and knowledge levels.

"For the purpose of implementing the proposed incident response actions, this Regulation establishes an EU Cybersecurity Reserve, consisting of incident response services from trusted providers, selected in accordance with the criteria laid down in this Regulation. Users of the services from the EU Cybersecurity Reserve shall include Member States' cyber crisis management authorities and CSIRTs and Union institutions, bodies and agencies. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve and may entrust, in full or in part, ENISA with the operation and administration of the EU Cybersecurity Reserve."

"The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States."

[44] https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy
[45] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
[46] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

The attestation scheme for cybersecurity skills aims to validate the technical skills and knowledge required for this role, fostering confidence in individuals performing these critical functions.

The PHOENI2X project, having already established communication channels with ENISA on this subject, proposed to coordinate discussions and feedback to ENISA on the Proposed 'Cyber Incident Emergency respondent' role profile from two projects (PHOENI2X and SYNAPSE), since all are working on the topic of Incident Response.

For the facilitation of the review of the proposed profile, a MIRO board was created.

Figure 36: MIRO board containing the tasks, knowledge and skills of the 'Cyber Incident Emergency respondent' (confidential)

The results were collected, consolidated and presented to ENISA on the 14th of April 2025.

5 STAKEHOLDER ENGAGEMENT AND LIAISON ACTIVITIES

This Chapter focuses on the outcome achieved by the engagement of various stakeholders to support the development of the PHOENI2X framework by providing feedback and valuable insights. Security Service Providers/Experts (SSPs/SSEs) and Critical Infrastructure Organizations (CIOs) were involved by responding to targeted surveys, while experts from various cybersecurity critical infrastructure sectors were interviewed.

The related activities were part of the Stakeholder Engagement Strategy devised during the 1st project period (M1-M18), aiming at leveraging stakeholders' expertise in the technical and business domains handled by the project, while increasing project visibility and raising awareness of a wider audience. During the 1st project period, the consortium analyzed the identified main stakeholders' interest, influence and power and then ranked and grouped them in Priority 1 and Priority 2 Stakeholder Groups. Based on this categorization, targeted engagement approaches were selected for each Stakeholder Group and a tailored engagement plan has shaped in Table 19 that was implemented successfully during the 2nd project period (M19 – M36).

Table 19 Engagement strategy for Stakeholder Groups (Priority 1 & Priority 2)

Stakeholder Group – Priority 1		Engagement Plan
Priority 1	Policy makers	At least 3 activities focusing on regulation and standards
	Partners of the PHOENI2X project	At least 5 **expert interviews**
	Critical Infrastructure Organizations (CIOs)	Exploring the needs and feedback of at least 3 (external to the project) CIOs through **targeted surveys**
	Security Service Providers/Experts (SSPs/SSEs) & EU-funded R&D projects	- Exploring the needs and feedback of 3 (SSPs/SSEs) through **targeted surveys** **- Liaison activities with R&D projects** (at least 3 joint activities)
Priority 2	Technology organizations (competitors)	- Invitations in at least 3 conferences/workshops - Participation in events with other stakeholders - Posts on the social media
	Other organizations	- Invitations in at least 3 conferences/workshops - Participation in events with other stakeholders - Posts on the social media
	Greater public	Dissemination activities (posts on the social media, project Newsletters, videos, etc.)

It should be noted that the engagement activities for Stakeholder Group – Priority 1 regarding (a) the liaison with other R&D projects and EC Initiatives have been reported in 2.2.4.3, and (b) regulation and standards have been reported in 2.2.4.3, while the engagement activities referring to the Stakeholder Group – Priority 2 have been already elaborated in 2.2.

5.1 Progress Highlights

5.1.1 Main achievements

During the second period of the project, the main achievements of PHOENI2X project in terms of stakeholders' engagement have been:

- The conduction of two (2) surveys addressing Security Service Providers/Experts (SSPs/SSEs) and Critical Infrastructure Organizations (CIOs) and the assessment of the collected input, and
- The conduction of seven (7) interviews with experts from various cybersecurity critical infrastructure sectors and the assessment of the collected input.

5.2 Stakeholders' engagement through targeted surveys and interviews

The main objective of the surveys and the interviews was to collect feedback on the PHOENI2X tools/solutions developed within the PHOENI2X framework to explore at what extent they meet the intended gaps and trends and whether there is any need for improvements in view of a potential commercialization. In addition, valuable insights were collected regarding key trends related to cybersecurity challenges, practices and priorities. Towards this end, two (2) customized questionnaires were created, one addressing the CIOs and another one addressing the SSP/SEs.

The surveys were provided over the online EUSurvey platform (EUSurvey - Documentation), a user friendly and intuitive online survey management tool compatible with most web browsers. Among its wide range of capabilities, the EUSurvey platform allowed us to respect the anonymity of the questionnaires participants (by selecting the 'Anonymous survey mode' option via the "security" section of the survey "properties"), as well as restrict participation through a password (by selecting the "secured" option via the "security" section of the survey "properties"), provided that we would address specific groups of participants. In addition, we were enabled to upload supportive files to accompany the surveys (e.g. a privacy notice and an informative presentation on the PHOENI2X scope, objectives, innovations, links, etc.) useful for the participants before they replied to the questions.

For both the surveys and the interviews the consortium followed a procedure (7) that ensured the protection of the participants' personal data and the anonymization and confidentiality of their responses as it had been already stated in the DMP D1.1. Specifically, (1) a Disclaimer was included at very beginning of the questionnaire before the introduction, (2) a Privacy Statement was included after the introduction and before the questions, (3) a Privacy Notice was sent to the selected contacts/stakeholders to inform them officially about the processing of their personal data (contact details and affiliation for the creation of the relevant contact list.

About the surveys:

For the surveys, two (2) dedicated invitation emails were sent to the stakeholders (a) SSPs/SEs, (b) CIOs, and (c) an invitation was posted on the LinkedIn).

Feedback was received from (30) SSPs/SEs and twenty-eight (28) CIOs. Both surveys (consisting of 20 and 18 Questions, respectively), - including ranking questions, multiple choice, Likert scales -, span across the following areas/parts:

- Profile/General
- Situational Awareness
- Response (Incident Response & Business Continuity)
- Preparedness
- Information Sharing
- Outro

The assessment of each part is quantitative. It includes diagrams, analysis of the results and key takeaways referring to: (a) the outcome of each question, (b) correlation between questions (where applicable) for each respondents' group (SEs and CIOs), and (c) comparison of the two groups' responses in case of common/similar questions. To facilitate comparison and where applicable, appropriate enumeration has been used to quantify the responses.

The key takeaways from the surveys and the interviews are provided in 5.3, whereas a more detailed exploration of the surveys' findings is provided in ANNEX 9 and ANNEX 10 (for SSPs/SEs and CIOs, respectively).

About the interviews:

The interviews were conducted in person or via videoconference, and their content was captured in written, fully anonymised form. Seven (7) interviews have been conducted. The interviewees contacted were experts from seven (7) cybersecurity critical infrastructure sectors: Railway, National Authority, Healthcare, Financial Exchange, Maritime, Telecommunications and Energy/Power.

The interviews were based on the following main questions:

Q1 (INT): When an organization is looking for a cybersecurity service provider, what key factors should they focus on to make the right choice?

Q2 (INT): Cyber threats and regulations are constantly evolving, what strategies do you use to ensure your security services stay up to date and compliant?

Q3 (INT): Different industries have unique security risks, how do you customize your services to meet the specific needs of different sectors?

Q4 (INT): How do you typically assess the success or effectiveness of the security solutions and services you deliver?

Additional questions investigated during one of the interviews:

Q5 (INT): What do you consider to be the main security hazards of critical infrastructures in the following years?

Q6 (INT): What do you consider to be the main improvements that should be implemented in the coming years to protect against these dangers?

The assessment of the interviews is qualitative based on the detailed responses of the interviewees.

The key takeaways from the interviews are provided in 5.4 and in some more details they can be found in ANNEXES.

Finally, a comparison of the findings from the surveys and the interviews is provided in 5.5.

5.3 Key takeaways from the surveys (addressing SSPs/SEs and CIOs)

The key takeaways of the surveys from both CIOs and SSPs/SEs are the following:

- Both groups identified external threats (e.g., cyberattacks) and internal errors & vulnerabilities as the **top concerns for cybersecurity**. Both groups ranked Non-compliance damages and BC/Client Satisfaction as the least important concern (Figure 37, see also Q3 (SEs) and Q4 (CIOs)).

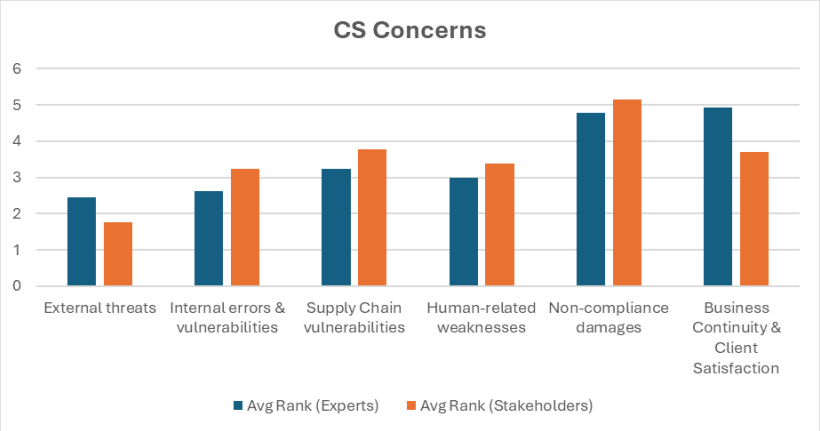


Figure 37: CS Concerns (SEs & CIOs)
(Top Concern: Rank 1 – Lowest Concern: Rank 3)

- Both groups highlighted cybersecurity funding and IR planning as **key challenges for improving CS**, followed by employee training and situational awareness (assets and threats). In addition, SEs placed greater emphasis on BC and both to translating cybersecurity into management terms as an important challenge (Figure 38, see also Q4 (SEs) and Q5 (CIOs)).

Figure 38: Key Challenges for CS (SEs & CIOs)

- Both groups agreed that cost of compliance, lack of internal expertise and regulatory complexity are **major compliance challenges**. In addition, CIOs emphasized management support (Figure 39, see Q18 (SEs) and Q15 (CIOs)).

Figure 39: Major Compliance Challenges (SEs & CIOs)

- Common **barriers for information sharing** across both groups have been considered the data security & privacy, the lack of strong relationships & trust between stakeholders, as well as legal and regulatory constraints (Figure 40, see also Q17 (SEs) and Q14 (CIOs)).

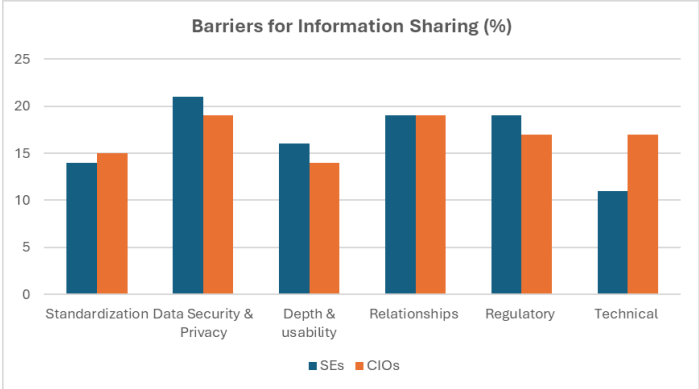


Figure 40: Barriers for Information sharing (SEs & CIOs)

- Both groups consider proactive & reactive incident response and security controls as **top priorities for CS improvement**. Moreover, CIOs focused also on local situational awareness, and SEs on BC & Resilience (Figure 41, see also Q19 (SEs) and Q18 (CIOs)).

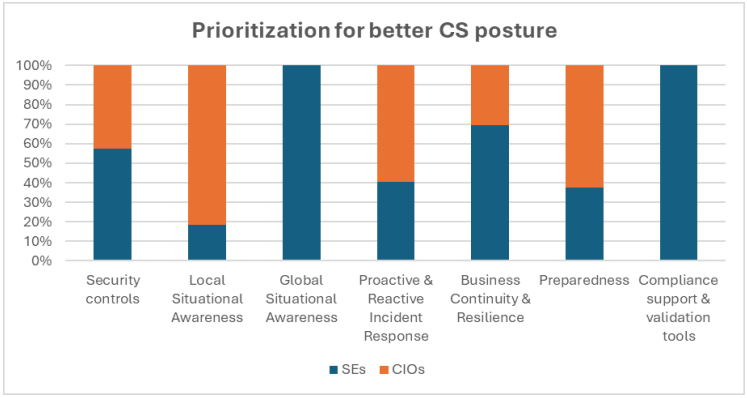


Figure 41: Top Priorities (SEs & CIOs)

- Regarding **situational awareness**, both groups ranked higher the real-time monitoring of cyber assets, along with vulnerability assessment and penetration testing. Solutions aggregating security events (e.g., SIEM) are also very important. **A surprising insight was the low prioritization or limited use of AI-based tools for situational awareness and for incident detection and threat hunting**. Currently, CIOs seem to prefer tried-and-tested tools over AI-based ones mainly due to cost barriers or lack of in-house expertise, while SEs address a gap in adopting advanced technologies for the same reasons (Figure 42, see Q6 (SEs) and Q10 (CIOs)).

Figure 42: Importance of Tools & Methods for Situational Awareness (SEs & CIOs)

- Regarding **resilience (IR & BC)**, both groups put top priority on the importance of tool access and place similar emphasis on resource allocation. SEs prioritize automation more than CIOs, whereas CIOs place greater emphasis on enhanced training & awareness. Both groups consider documentation as the least important aspect (Figure 43, see also Q11 (SEs) and Q11 (CIOs)).

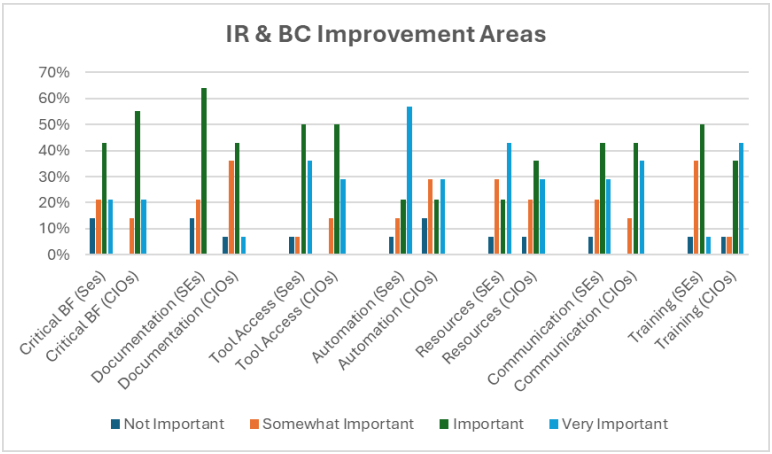


Figure 43: Importance of Aspects for IR & BC (SEs & CIOs)

- Concerning the **learning methods**, both groups strongly favored interactive and hands-on training such as seminars, tabletop exercises and realistic simulations. However, SEs indicate alignment in priority but differences in implementation capacity, widely adopting Seminars and workshops and Self-study material. Serious games remain a less developed method across both groups (Figure 44, see Q12 (SEs) and Q12 (CIOs)).

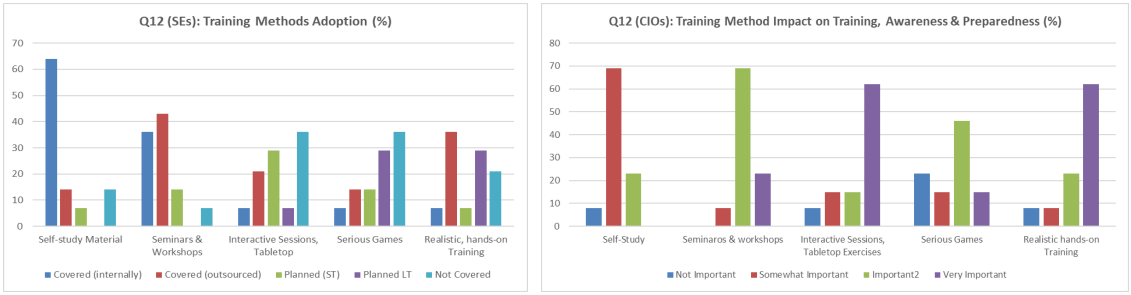


Figure 44: Learning Methods Adoption & Impact (SEs & CIOs)

- Among the **Cybersecurity Frameworks (CSF),** ENISA/EU Cybersecurity Certification has been prioritized by the CIOs, followed by the NIST CSF which was identified by the SEs as the most popular one (Figure 45, see also Q5 (SEs) and Q7 (CIOs)).

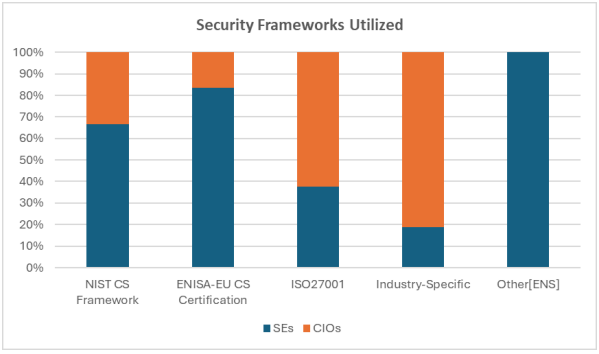


Figure 45: Security frameworks Utilized (SEs & CIOs)

- As **major areas of impact of the PHOENI2X framework** both groups acknowledged training & awareness and enhanced alerting. In addition, CIOs placed slightly greater emphasis on BC & IR (Figure 46, see also Q20 (SEs) and Q17 (CIOs)).

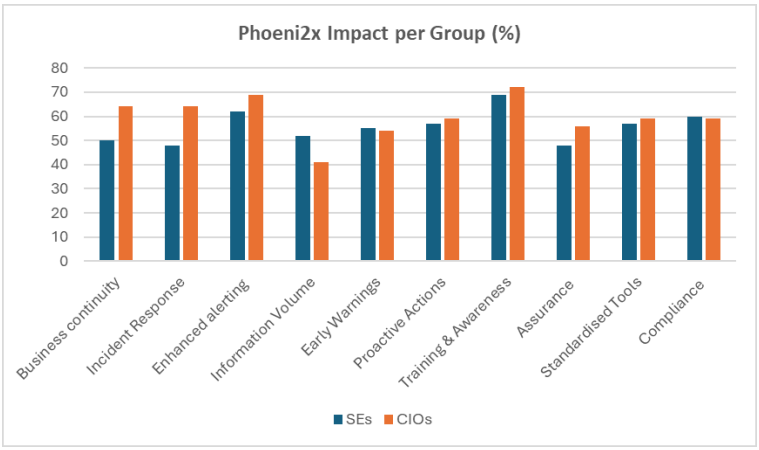


Figure 46: Security FPHOENI2X Areas of Impact (SEs & CIOs)

As PHOENI2X progresses towards its final phases, the feedback obtained from the surveys serves as a testament to its impactful contributions to the cybersecurity domain. The project's holistic approach, encompassing technological innovation, strategic training and collaborative information sharing, positions it as a cornerstone in fortifying Europe's cyber infrastructure.

5.4 Key takeaways from the targeted interviews

This section highlights the main insights from interviews conducted with cybersecurity professionals across seven critical sectors: National Cybersecurity Authority, Financial Exchange, Telecommunications, Naval, Healthcare, Railway and Power.

It can be seen that while cybersecurity fundamentals (security principles, success measurement approaches and training preferences) remain consistent across sectors, each critical infrastructure domain has specific operational conditions (unique performance requirements, faces specialized threats, operates within specific regulatory frameworks, demonstrates varying technology adoption patterns) that share common characteristics/metrics. As a result, critical infrastructure cybersecurity requires a sophisticated understanding of both universal cybersecurity principles and sector-specific security principles and the cybersecurity effectiveness depends on this deep understanding and not simply on technical capabilities.

The interviews showcased the following key takeaways, mainly valid across all the interviewed sectors:

- Regarding the service provider selection criteria, all sectors focus mainly on (a) sector-specific expertise (with proven track record) and understanding of industry-specific requirements, (b)

reputation and client references, as well as (c) regulatory compliance and relevant certifications on the sector-specific standards.

- All sectors perform actions towards staying current with evolving threats, utilizing common strategies such as: continuous threat intelligence, regulatory monitoring (complying with their sector-specific and horizontal regulations), utilization of security tools incl. real-time monitoring systems, and professional development through ongoing training, awareness and certification programs.
- All sectors noted that they follow sector-specific regulations and standards. Common among all are the NIS2 directive, GDPR compliance and ISO 27001 family regarding information security management.
- All sectors stated that security challenges regard multiple regulations and standards need to be followed, to comply with the sector-specific standards, and those in many cases can be overlapping. Moreover, third-party vendors and systems must be extensively tested before utilized (especially highlighted in the Maritime sector).
- Most sectors utilize identity-based access controls and network segmentation techniques as their technology focus area, with Healthcare focusing in addition on communication and data protection.
- All sectors share their own success measurement frameworks and KPIs to constantly assess their effectiveness. Common metrics across most sectors include Response Metrics such as response time, as well as compliance scores and audit results.
- AI/ML adoption/integration is emerging across sectors to address evolving threats and regulatory requirements but not yet fully implemented due to cost and expertise constraints. Telecommunication sector shows the most advanced AI adoption (AI-driven anomaly detection, threat intelligence), while Healthcare appears to be falling rather behind in AI adoption, with no mention of AI/ML technologies in their cybersecurity strategies. Railway has limited adoption of AI-driven security tools, while Energy, Authority and Maritime Sectors have adapted AI-driven threat detection and automated response systems.

Generally, via the interviews it can be noticed that Telecommunications shows the most advanced technology adoption overall, Railway has unique legacy infrastructure challenges, Maritime has the most comprehensive vendor security requirements, Financial Exchange emphasizes performance requirements (latency, availability) and finally, National Authority has the broadest regulatory oversight responsibilities.

PHOENI2XWhile cybersecurity fundamentals remain consistent across sectors, each critical infrastructure domain has unique requirements, threats and regulatory frameworks.

5.5 Comparative findings from the surveys and the interviews

The cross-analysis between questionnaires (by the CIOs and SEs groups) and interviews reveals strong alignment between questionnaire findings and interview insights, validating the critical challenges and priorities identified by both CIOs and SEs while providing deeper sector-specific context and implementation details.

- Both CIOs and SEs identified regulatory complexity and compliance costs as major obstacles for CS improvement, which is supported by the interview's findings. ENISA/EU Cybersecurity Certification, NIST CSF and sector/industry-specific standards emerged as top-ranked frameworks by all the involved stakeholders. The interviews mentioned also overlapping issues and strict regulatory, sector-based requirements. In addition, most sectors have assigned dedicated compliance teams for continuous regulatory monitoring.

- Both groups identified external threats (cyberattacks) and internal errors & vulnerabilities as top concerns for the CS posture, which was also validated across all sectors. In addition, Healthcare and Energy sectors particularly highlighting human-related vulnerabilities, while Financial and Telecom sectors emphasized sophisticated insider threat detection.
- Both groups highlighted funding for CS as a key challenge, along with lack of internal expertise and management support. The interviews confirmed across all sectors the importance of specialized expertise (e.g. rail-specific protocols, maritime vessel systems and ICS/SCADA knowledge).
- Common challenge across both groups was communication and data-sharing limitations, along with technical barriers and privacy concerns. The interviews revealed multi-stakeholder collaboration challenges due to regulatory constraints, interoperability issues with sector-specific protocols, and trust barriers between stakeholders.
- Both groups consider proactive & reactive incident response as top priorities, along with situational awareness and compliance tools. The interviews are also aligned by highlighting the importance of 24/7 monitoring operations with sector-specific threat intelligence sources.
- Both groups and interviews emphasized real-time monitoring and SIEM/ROAR solutions as very important as well as relevant AI/ML tools. However, AI-based tools emerge as a trend but with limited usage in the current landscape.
- Both groups strongly favored interactive, hands-on training such as seminars and tabletop exercises, as well as realistic training. The interviews indicated industry-specific training programs, like seminars and workshops (incl. maritime GPS jamming scenarios, healthcare patient data protection and railway safety-critical system education).
- Both groups acknowledged training & awareness and enhanced alerting as major PHOENI2X impact areas, as well as business continuity, proactive actions and compliance improvements. The interviews support this holistic approach through comprehensive cybersecurity solutions, technology innovation and multi-stakeholder collaboration across strategic and operational levels.

The consistency of findings may provide strong evidence that real market needs have been addressed and some strategic recommendations could be drawn for the PHOENI2X framework to prioritize to enhance its commercialization potential across multiple essential service industries:

1. Modularity: Adaptable to sector-specific needs
2. Compliance: Multi-framework regulatory support
3. Performance: Scalable to different operational requirements
4. Intelligence: Cross-sector threat correlation and prediction (based on AI/ML)
5. Usability: Stakeholder-appropriate interfaces and workflows

Based on the above, the success of the PHOENI2X framework will depend on its ability to serve as both a flexible, modular platform that provides universal security capabilities while enabling sector-specific customization without compromising core security effectiveness. The key differentiator will be the ability to correlate threats and best practices across sectors while respecting the unique operational and regulatory requirements of each industry.

6 CLOSING REMARKS

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), carried out during the end period of the project (M18-M36).

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

In relation to Communication & Dissemination, the project carried out the dissemination and communication plan designed at the beginning of the project. The dissemination and communication KPIs of the project were reached and the project message and results were effectively communicated. Different activities based on the type of stakeholders were implemented ranging from conference publications and presentations to participation in Summer schools and training event.

In relation to Impact creation, Exploitation & Standardisation activities, discussions have taken place to gather information on the exploitation potential of the project solution and its components. The project (from the 1st period of the project) has identified 5 Key Exploitable Results (KERs). For these KERs, following the initial identification of the market, its size, the potential, the key players and issues (carried out during the 1st period), individual exploitation analysis was carried out and a draft joined exploitation plan for the PHOENI2X solution / service was agreed and documented. The initial potential (strengths and opportunities) and issues (threats and weaknesses) were reviewed, updated based on the feedback of tasks 5.4 and 6.3 and were documented. The PHOENI2X solution / service resides at TRL 4 at the end of the project, so immediate exploitation is not possible, but the partners have initially agreed on possible next steps and approaches regarding exploitation and commercialization.

In relation to Stakeholder Engagement and EC Initiatives' Liaisons, the methodology introduced in the 1st period of the project, was followed and results were extracted. Different engagement activities were carried out, including interviews and surveys, and results on their needs and expectations in relation to the key topics of the project were extracted. The results of these activities are recorded within Section 5 of this document.

7 ANNEX - Protection of personal data, anonymization and confidentiality of the response to the surveys

To ensure the protection of the participants' personal data and the anonymization and confidentiality of their responses, the consortium proceeded with the following steps:

1. The following Disclaimer was included at the beginning of the questionnaire before the introduction:

The European Commission is not responsible for the content of questionnaires created using the EUSurvey service - it remains the sole responsibility of the form creator and manager. The use of EUSurvey service does not imply a recommendation or endorsement, by the European Commission, of the views expressed within them.

2. The following Privacy Statement was included after the introduction and before the questions:

The information provided in this questionnaire is crucial for the PHOENI2X project (https://www. https://PHOENI2X.eu). Any data provided will be treated with the utmost confidentiality and will comply with applicable data protection laws such as the EU's General Data Protection Regulation (GDPR). Based on your consent, the data collected will be used under stringent data protection measures such as encryption and access control to gather valuable information relevant to the PHOENI2X solution strictly for research and project development purposes. The information collected will be stored securely on the EUSurvey platform and the project's private online repository at the ownCloud platform and will be accessible only to authorized project personnel. We will retain your data only for the duration necessary for the project and will ensure its secure deletion or anonymization thereafter and at the latest within one year after the completion of the project. No automated decision-making based on your data will be performed. You have the right to access, rectify, transfer, delete, or restrict the processing of your data, or withdraw consent at any time by contacting our Project Coordinator (Kostas Lampropoulos, email: klamprop@ece.upatras.gr). You have the right to lodge a complaint with the supervisory authority of the member state of your habitual residence or place of an alleged infringement of the GDPR. By providing your data, you acknowledge and agree to these terms.

3. The following Privacy Notice was sent to the selected contacts/stakeholders to inform them officially about our collecting their personal data (contact details and affiliation) for the specific stakeholders' engagement activities and provided all the necessary information in accordance with GDPR. The same Privacy Notice was included in the mail distributing the survey link to eliminate any doubt as to whether the participants had been already informed:

As the PHOENI2X project consortium (https://www. https://PHOENI2X.eu), we are committed to respecting your privacy. The purpose of this notice is to inform you about the processing of your personal data in accordance with art 14 of the GDPR. The personal data we have collected were provided by the project partners and consist of your contact details (name, email address) and affiliation (organization, position). Based on our legitimate interest in promoting the project and its outcomes, we intend to use your data to communicate with you solely about the project's stakeholder engagement activities, including contacting you to arrange an interview or sharing with you a survey to elicit information about the PHOENI2X solution, its innovations, commercialization potential, and the need for improvements. We have securely stored your data on the ownCloud platform and will not share them with any other parties external to the consortium. We will retain your data strictly for the project's duration. No automated decision-making based on your data will be performed. You have the right to access, rectify, transfer, delete, restrict and object to the processing of your personal data. To exercise your rights, or in case you wish to not receive any emails from us, please contact our Project Coordinator (Kostas Lampropoulos, email: klamprop@ece.upatras.gr). If you remain unhappy with how we have used your data after raising a complaint with us, you can also lodge a complaint with the

supervisory authority of the member state of your habitual residence or place of an alleged infringement of the GDPR.

8 ANNEX – Invitations for the surveys

The two (2) dedicated invitation emails that were sent to the stakeholders (a) SSPs/SEs, (b) CIOs, (c) and the post on the LinkedIn were the following:

(a) Email to the SSPs/SEs:

Dear Sir/Madam,

We are pleased to invite you to contribute to the EU-funded R&D project PHOENI2X by sharing your expertise through a short, 15-minute survey for SEs (password: @PHOENI2X@). The survey has been designed to assess the Cyber Resilience Framework currently under development within the project.

*Your insights will be invaluable in advancing and evaluating the PHOENI2X project, which aims at providing **Artificial Intelligence (AI)-assisted orchestration, automation and response capabilities for business continuity, incident response and information exchange**. The PHOENI2X Framework is tailored to meet the needs of Operators of Essential Services (OES) and EU Member State (MS) National Authorities responsible for cybersecurity.*

*The survey will remain open until **December 31, 2024** and all responses will be treated confidentially, used solely for research purposes. For more details on data handling, please refer to our **Privacy Notice**.*

We greatly appreciate your participation and support in this important initiative.

For further information, feel free to contact us, visit the project website, or follow us on social media (X, Facebook, LinkedIn).

Thank you in advance for your valuable contribution.

Best Regards,

The PHOENI2X Team

(b) Email to the CIOs:

Dear Sir/Madam,

We are pleased to invite you to contribute to the EU-funded R&D project PHOENI2X by sharing your expertise through a short, 15-minute survey for CIOs (password: @PHOENI2X@). The survey has been designed to assess the Cyber Resilience Framework currently under development within the project.

*Your insights will be invaluable in advancing and evaluating the PHOENI2X project, which aims at providing **Artificial Intelligence (AI)-assisted orchestration, automation and response capabilities for business continuity, incident response and information exchange**. The PHOENI2X Framework is tailored to meet the needs of Operators of Essential Services (OES) and EU Member State (MS) National Authorities responsible for cybersecurity.*

*The survey will remain open until **December 31, 2024** and all responses will be treated confidentially, used solely for research purposes. For more details on data handling, please refer to our **Privacy Notice**.*

We greatly appreciate your participation and support in this important initiative.

For further information, feel free to contact us, visit the project website, or follow us on social media (X, Facebook, LinkedIn).

Thank you in advance for your valuable contribution.

Best Regards,

The PHOENI2X Team

(c) Post on the LinkedIn (https://www.linkedin.com/posts/PHOENI2X_the-members-of-the-PHOENI2X-consortium-are-activity-7274405989729075200-rR0Q?utm_source=share&utm_medium=member_desktop&rcm=ACoAAABvHQgBWHaI82n3ZBFNrwLD-1gNYo7W7m8) Figure 47) to attract more participants:

The members of the PHOENI2X Consortium are pleased to invite you to contribute to the EU-funded R&D project PHOENI2X by sharing your expertise through a short, 15-minute survey.

The survey has been designed to assess the Cyber Resilience Framework currently under development within the project.

If you work for a Critical Infrastructure Organization (CIO), then you can utilize the link: survey for CIOs (password: @PHOENI2X@).

If you are a Security Service Provider and/or consider yourself as a Security Expert, then you can utilize the link: survey for SEs (password: @PHOENI2X@).

Your insights will be invaluable in advancing and evaluating the PHOENI2X project, which aims at providing Artificial Intelligence (AI)-assisted orchestration, automation and response capabilities for business continuity, incident response and information exchange. The PHOENI2X Framework is tailored to meet the needs of Operators of Essential Services (OES) and EU Member State (MS) National Authorities responsible for cybersecurity.

The survey will remain open until January 31, 2025 and all responses will be treated confidentially, used solely for research purposes. For more details on data handling, please refer to our Privacy Notice.

We greatly appreciate your participation and support in this important initiative.

For further information, feel free to contact us via the project website (https://PHOENI2X.eu/contact/).

Thank you in advance for your valuable contribution.

The PHOENI2X Team

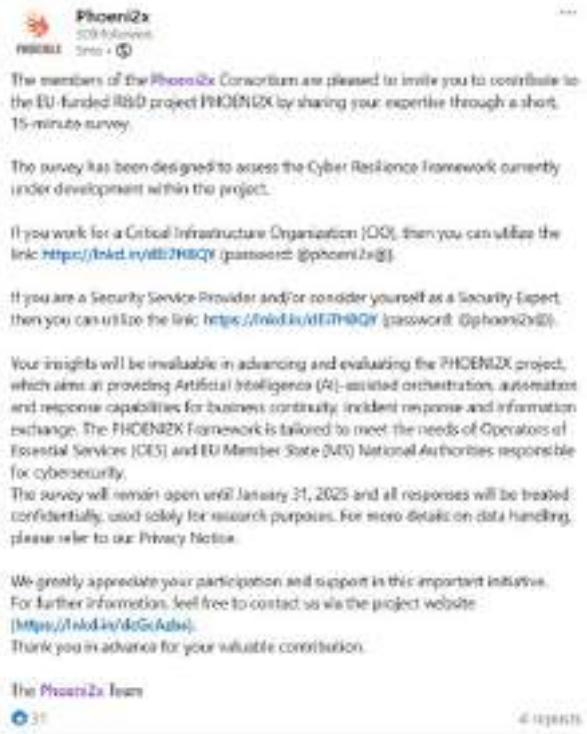


Figure 47: Invitation for participation in the surveys posted on the LinkedIn

9 ANNEX – Insights and feedback derived from SSPs/SEs

The survey addressing the SSPs/SEs comprises the following parts:

- Profile/General: Q1 – Q5 9.1
- Situational Awareness: Q6 - Q7 9.2
- Response (Incident Response & Business Continuity): Q8 - Q11 9.3
- Preparedness: Q12 - Q14 9.4
- Information Sharing: Q15 - Q17 9.5
- Outro: Q18 – Q20 9.6

9.1 Profile/General (SEs)

Q1. Which sector does your organization operate in? (Please select the most relevant) (Common to Q2 (CIOs))

Energy; Telecommunications; Transportation Systems; Healthcare; Information Technology; Financial Services; Other [Government, Maritime, Higher Education, TIC[47]]

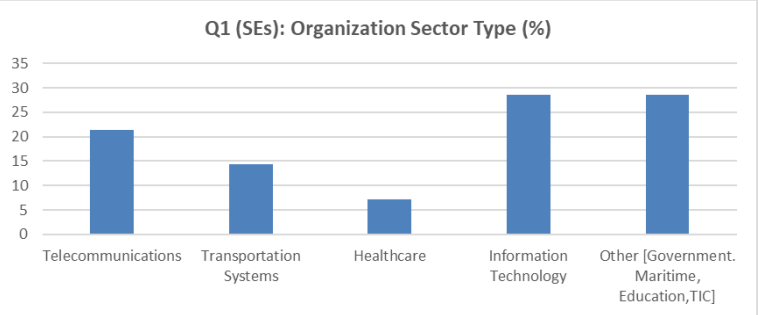


Figure 48: (SEs) Organization Sector Type (%)

Q2. What is your role within your organization? (Common to Q3 (CIOs))

CEO/Director; CIO/CTO; CISO; Team Lead/ Manager; IT personnel; Other [e.g. Field CISO, Professor]

Figure 49: (SEs) Role Distribution

[47] Testing, Inspection, Certification body

Among the 30 SEs, the majority were Managers/Team Leaders and secondarily, IT personnel, CISO, Other (e.g. Field CISO, Professor).

Q3. Please rank the following concerns in order of importance, from your perspective, when it comes to the cybersecurity of your organization's infrastructure. (Rank answers) (Common to Q4 (CIOs))

External threats; Internal errors & vulnerabilities; Supply Chain vulnerabilities; Human-related weaknesses; Non-compliance damages; Business Continuity & Client Satisfaction

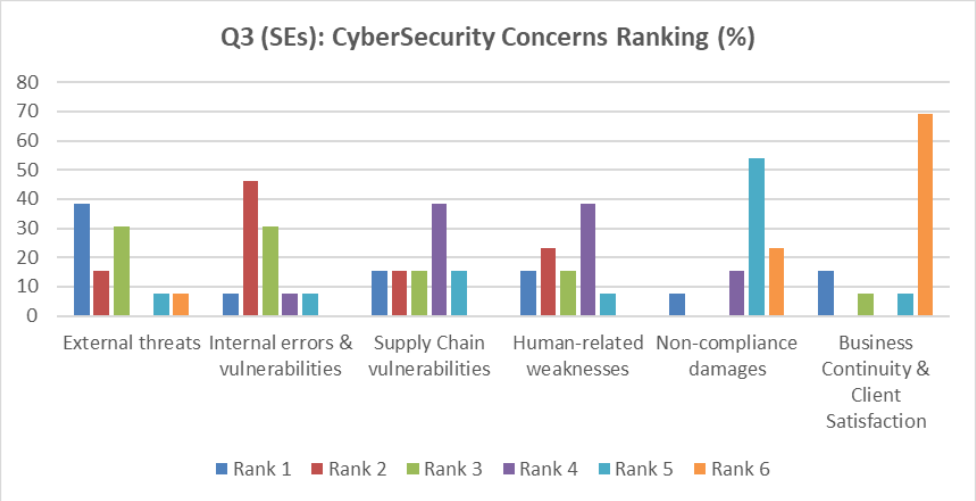


Figure 50: (SEs) Cybersecurity Concerns Ranking (%)

The external threats were ranked as top concerns (Rank 1) by the SEs.

In more details:

- Rank 1: The most pressing concerns for organizations are external threats from outside their environment (such as hackers, malware, ransomware, and cyberattacks). This may reflect the increasing volume and sophistication of cyberattacks in the global landscape and suggests that organizations must prioritize defense against external attacks accordingly by prioritizing investments in prevention, detection, and response capabilities focused on external threats.

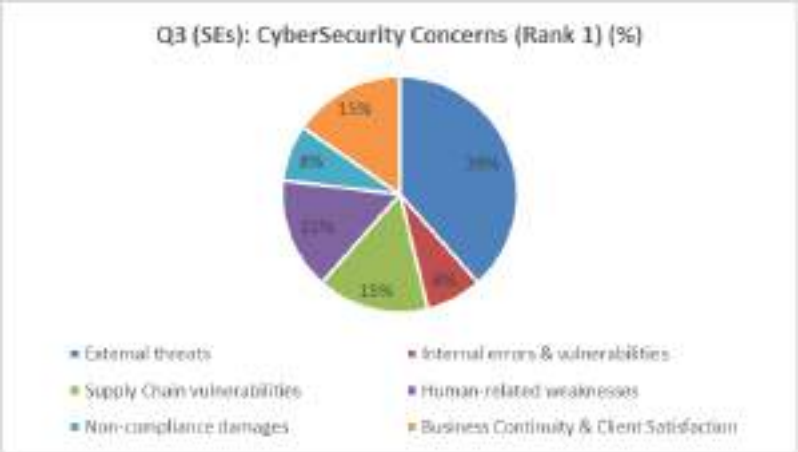


Figure 51: (SEs) CyberSecurity Concerns (Rank 1) (%)

- Rank 2: Internal vulnerabilities (e.g., misconfigurations, poor security hygiene, or malicious insiders) represent significant risks; thus, pointing to the necessity of improving internal security practices such as employee training and the use of automated monitoring tools to identify potential weaknesses.
- Rank 3: The important concern over supply chain vulnerabilities emphasizes the growing need for expanding security posture beyond own systems to include third-party vendors, as a critical risk factor in today's interconnected landscape.
- Rank 4: Human-related weaknesses remain a substantial concern, stressing the need for more advanced training methods (e.g., simulations, cybersecurity exercises) and continuous reinforcement of security best practices across the organization.
- Rank 5 & Rank 6: Non-compliance and business continuity are important but not urgent. However, organizations should be aware that non-compliance could eventually lead to significant regulatory or financial consequences (particularly as new regulations such as GDPR and NIS2 are introduced in the EU), while business continuity should remain part of longer-term strategic plans.

Q4. Please assess each of the below limitations & challenges in terms of the extent that they may hinder your organisation's ability to further improve its cybersecurity posture. (Please select importance of each option; selection from Not an issue/Minor issue/Important issue/Major issue) (Common to Q5 (CIOs))

- Difficulty in maintaining situational awareness and visibility in terms of the assets (IT/ OT/ IIoT[48]) in your infrastructure & their status
- Difficulty in maintaining situational awareness and visibility in terms of pertinent threats that affect you and your peers (threat intelligence)
- Inadequate incident response planning
- Lack of access to relevant cyber-defence tools & technologies
- Difficulty in securing funding to be invested in cybersecurity
- Business continuity planning & implementation
- Translating cybersecurity issues
- Lack of employee training & awareness
- Lack of access to information exchange mechanisms

[48] Information technology/ Operational Technology/ Industrial Internet of Things

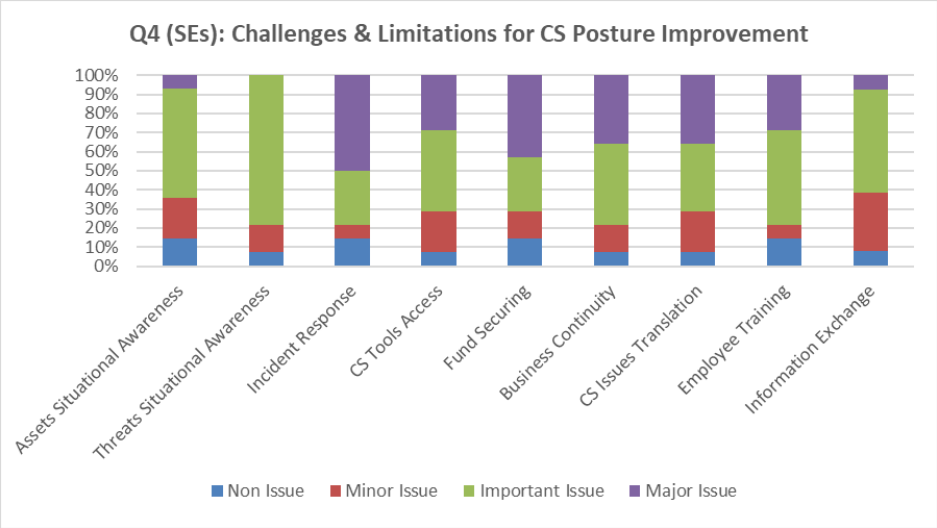


Figure 52: (SEs) Challenges and Limitations for CS Posture Improvement

Most of the SEs respondents ranked the inadequate incident response planning and the difficulty in securing funding to be invested in cybersecurity as the major challenges. The difficulty in maintaining situational awareness and visibility in terms of the threat intelligence was ranked as an important one.

Q5. What security frameworks and/or standards do you primarily follow in your organization? (Please select all that apply) (Similar to Q7 (CIOs))

- NIST Cybersecurity Framework (CSF)
- ENISA/EU Cybersecurity Certification
- ISO27001 family of standards (please specify) | 27001:2013, 27002:2013, 27003:2017, 27005:2018, 27011:2016, Information management practices
- Industry-specific (e.g., ISA/IEC 62443, HIPAA, PCI-DSS; please specify) | IACS, Automotive, Embedded, Rail industry
- Other [ENS[49]]

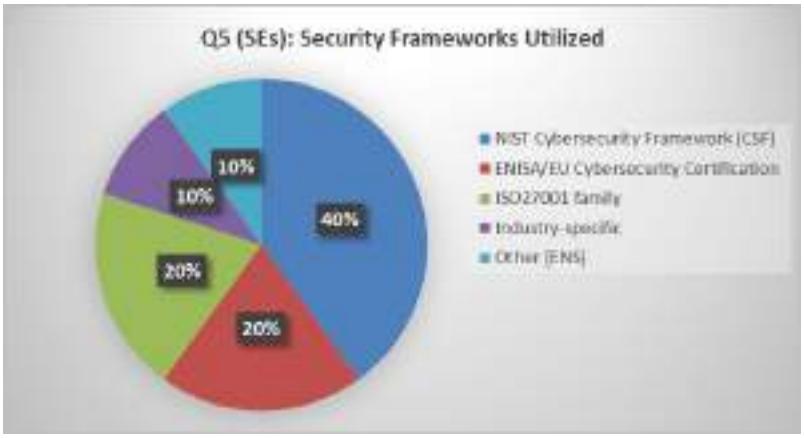


Figure 53: (SEs) Security Framework Utilized

The NIST Cybersecurity Framework (CSF) was identified by the SEs as the most popular one.

[49] Esquema Nacional de Seguridad (Spanish National Security Framework)

9.2 Situational Awareness (SEs)

Q6. Please rank the following approaches, tools & methods in terms of importance in providing your organisation with situational awareness regarding cyber threats. (Similar to Q10 (CIOs))

Vulnerability Assessments; Penetration Testing; Real-time monitoring of cyber assets; Solutions aggregating security events in real time; Access to timely and relevant CTI information; AI-based tools; Risk-focused impact assessment; Other

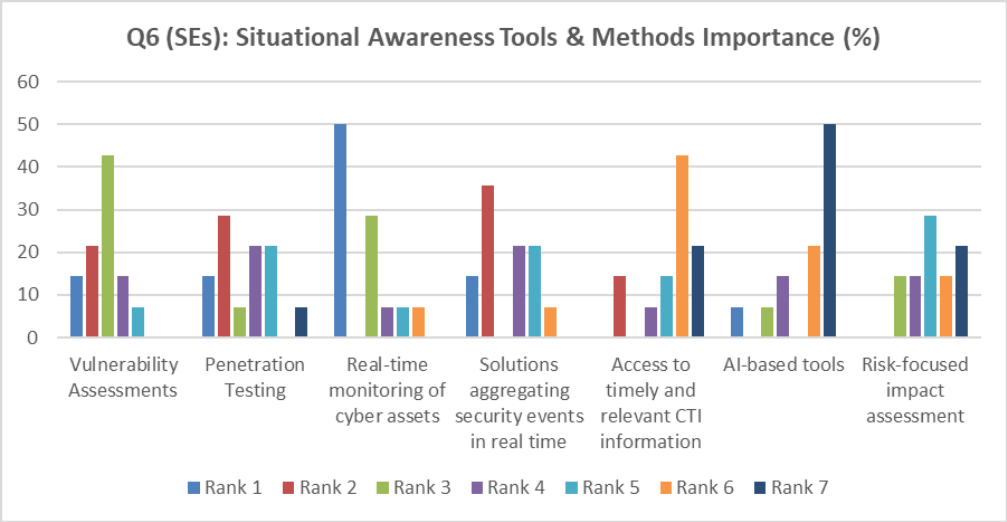


Figure 54: (SEs) Situational Awareness Tools and Methods Importance (%)

Figure 55: (SEs) Situational Awareness Tools and Methods Importance (Avg Rank)

Real-time monitoring was ranked as the most important method in providing situational awareness regarding cyber threats.

In more details:

- **Real-time monitoring** highest ranking highlights the need for continuous visibility into systems and assets. This is likely driven by the growing complexity and speed of cyber threats, which require immediate detection and mitigation.
- **Traditional methods like vulnerability assessments and penetration testing** remain foundational to cybersecurity for identifying and addressing system vulnerabilities, despite the advent of new technologies.

- **Event aggregation solutions** (e.g., SIEM) are equally important as traditional testing methods, as they provide an integrated view of security events across the network, which is essential for a timely response to potential threats.
- **AI-based tools** are not yet as central to cybersecurity practices as other methods, possibly due to concerns about their maturity, complexity and the need for skilled personnel to implement them effectively. However, they are still seen as useful supplementary tools.
- **Threat intelligence and risk assessments** are valuable but considered less urgent. While these approaches provide insight into the external threat landscape and potential impacts, they may not be as immediately actionable as real-time data from internal systems.

Q7. How often are the following approaches, tools & methods for situational awareness being used within your organisation?

- Vulnerability Assessments
- Penetration Testing
- Real-time monitoring of cyber assets
- Solutions aggregating security events in real time
- Access to timely & relevant CTI
- AI-based tools for enhanced incident detection, attack prediction & threat hunting
- Risk-focused impact assessment of identified threats

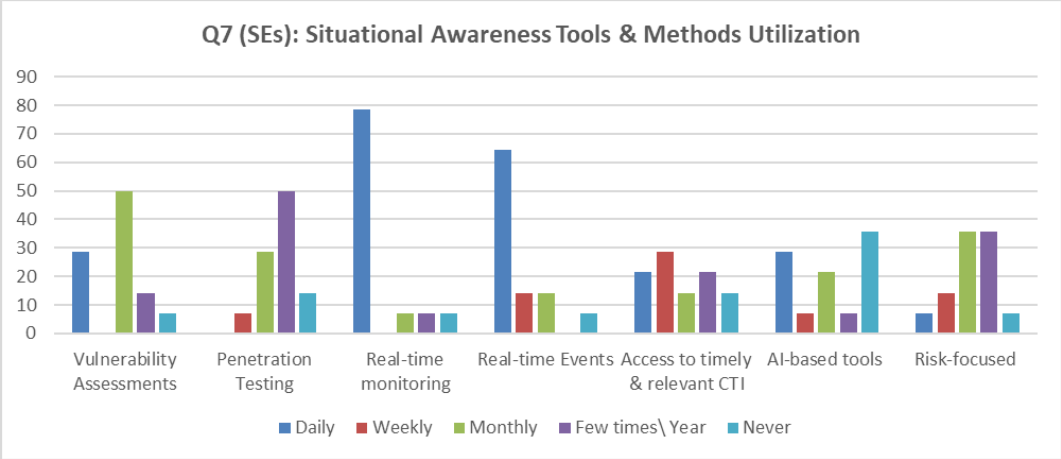


Figure 56: (SEs) Situational Awareness Tools and Methods Utilization

Both real-time monitoring and aggregating solutions are mainly used and are performed on a daily basis.

9.3 Response (Incident Response & Business Continuity) (SEs)

Q8. Which of the following Incident Response measures does your organization currently have in place? (Select all that apply)

- Incident detection, orchestration & response systems/tools
- Incident response team
- Pre-defined incident response procedures
- Incident tracking and reporting mechanisms

- Communication plans for internal and external stakeholders
- Post-incident analysis and lessons learned reviews
- Regular incident response drills and exercises
- External partnerships for incident response support

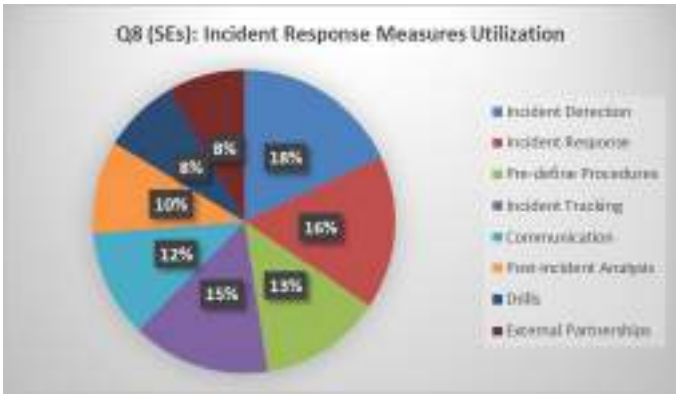


Figure 57: (SEs) Incident Response Measures Utilization

Incident detection/orchestration/response systems, Incident Response team and Incident tracking and reporting mechanisms are the three (3) most utilized Incident Response measures.

Q9. Which of the following Business Continuity measures does your organization currently have in place? (Select all that apply)

- Regular data backups
- Off-site data storage
- Redundant systems and failover mechanisms
- Disaster recovery sites
- Regularly updated Business Continuity Plan (BCP)
- Business impact analysis
- Risk assessment and management
- Employee training and awareness programs
- Communication plans for internal and external stakeholders

Figure 58: (SEs) Business Continuity Measures Utilization

Regular data backups, Redundant systems and failover mechanisms and Employee training and awareness programs are the three (3) top Business Continuity measures utilized.

Q10. Which of the following components / functionalities would you prefer to have within an Incident Response & Business Continuity software? (Select all that apply)

- Procedures depicted in the form of static workflow
- Procedures presented in no-code, editable graphs
- Executable Playbooks
- Shared early notification information
- Scenario Simulation Ability
- Embedded logic within the playbook software

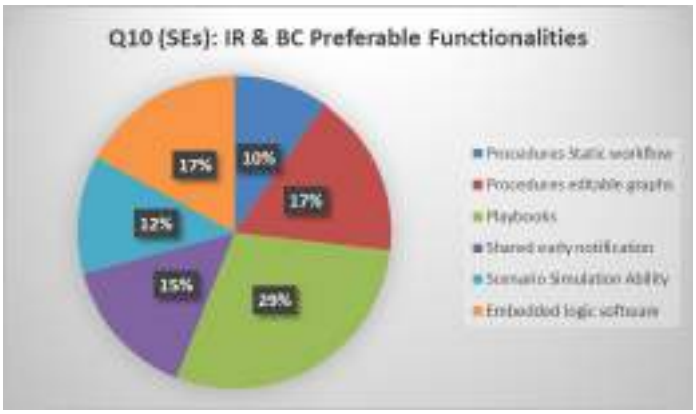


Figure 59: (SEs) IR and PC Preferable Functionalities

The executable playbooks were by far the most preferable components within an Incident Response & Business Continuity software.

Q11. Rate the following areas in terms of importance for improving your current Incident Response and Business Continuity practices & maturity. (Common to Q11 (CIOs))

- More effort on identifying critical business functions & maintaining up to date plans.
- More comprehensive planning and documentation, including encoding relevant processes in the form of structured workflows (e.g., playbooks).
- Improved access to relevant tools (e.g., for data availability and integrity, monitoring, incident detection)
- Adoption of Automation, Orchestration & Response technologies.
- Allocation of more resources (e.g., budget)
- Better communication and coordination during incidents.
- Enhanced Training & Awareness programs, including tests & drills, on relevant processes.

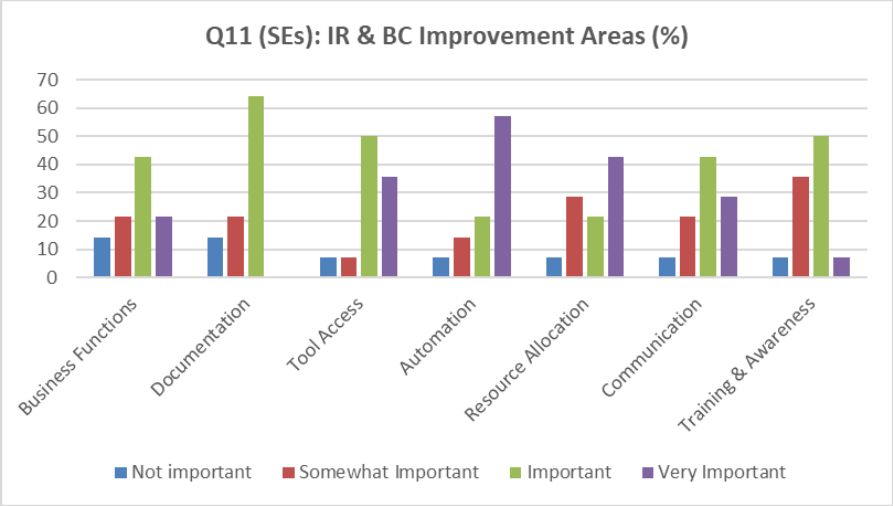


Figure 60: (SEs) IR and BC Improvement Areas (%)

Figure 61: (SEs) IR and BC Improvement Areas (*)

(*) Used Enumeration: Not Important: 0, Somewhat Important: 1, Important: 3, Very Important: 5

All the above areas (excluding the Training & Awareness) share more or less the same level of importance as far as improving IR and BC practices and maturity.

9.4 Preparedness (SEs)

Q12. Considering the different types of training delivery methods listed below, please select the current adoption status within your organisation. (Similar to Q12 (CIOs))

Self-study material provision (e.g., brochures, newsletters, literature); Seminars & Workshops; Interactive Sessions, Tabletop Exercises; Serious Games; Realistic, hands-on Training

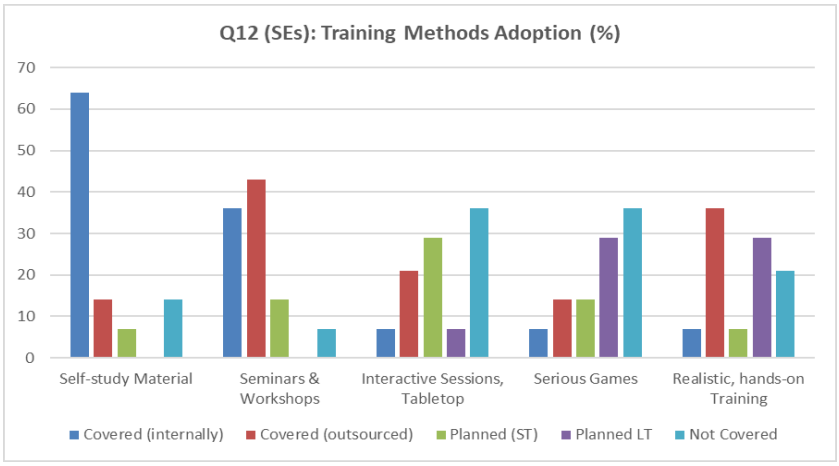


Figure 62: (SEs) Training Methods Adoption (%)

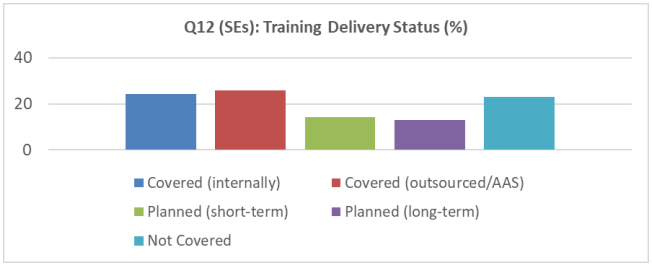


Figure 63: (SEs) Training Delivery Status (%)

- The most adopted training method is Self-study, primarily covered internally.
- Seminars & Workshops are also well-covered, split between internal and outsourced delivery.
- Interactive Sessions and Serious Games show a gap between actual adoption and intention for adoption, with many responses marked as "Planned (short/long term)" but not yet widely implemented.
- Realistic, hands-on training is relatively more common in outsourced form, suggesting possible resource or expertise limitations for internal execution.

Q13. Considering the different types of training topics mentioned below, please specify the means of delivery of training sessions, if any, carried out within your organisation.

- Basic cybersecurity training (basic cyber-hygiene, recognising & reporting)
- Technical training on situational awareness topics
- Training on Cyber Threat Intelligence
- Training on Incident Response & post-Incident Analysis topics & processes
- Training on Business Continuity topics & processes
- Training on collaboration, coordination & alerting and reporting topics & processes

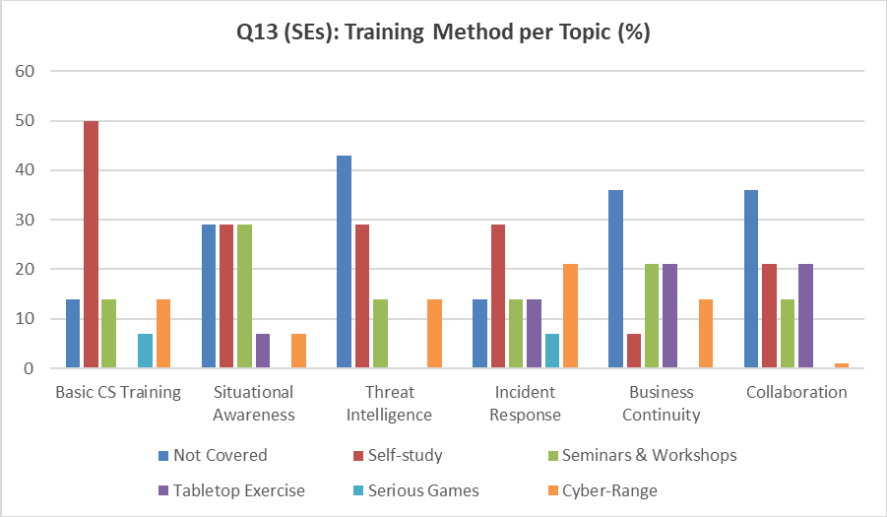


Figure 64: (SEs) Training Method per Topic (%)

Figure 65: (SEs) Training Procedures Utilized

Once again (like in Q12 (SEs)), the most common method across all topics is Self-study, indicating a reliance on individual learning. Overreliance on this method, although cost-effective, may be insufficient for complex topics like Incident Response or Threat Intelligence. Advanced and interactive training methods (Cyber-Ranges, Serious Games, Tabletop) are less frequently utilized, perhaps signaling a potential gap between topic complexity and delivery effectiveness, while the low utilization of hands-on training may suggest a skills gap in hands-on experience, which is critical in real cyber incidents.

Q14. Considering the different types of training topics mentioned below, please specify the frequency of training sessions carried out within your organisation

- Basic cybersecurity training
- Technical training on situational awareness topics
- Training on Cyber Threat Intelligence
- Training on Incident Response & post-Incident Analysis topics & processes
- Training on Business Continuity topics & processes
- Training on collaboration, coordination & alerting and reporting topics & processes

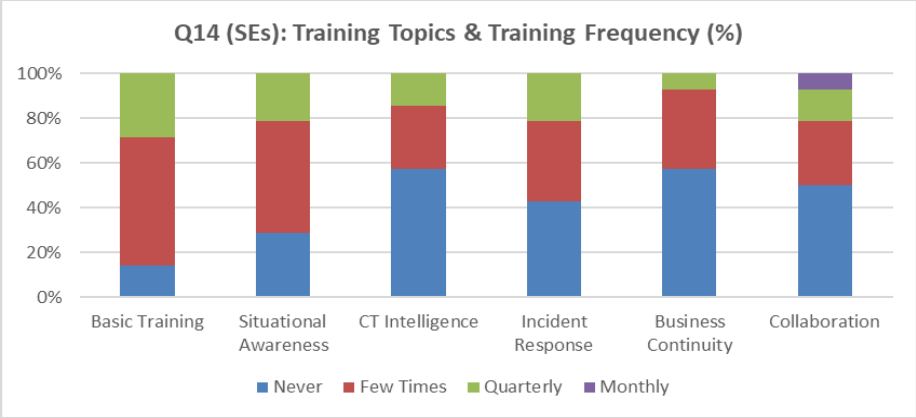


Figure 66: (SEs) Training Topics and Training Frequency (%)

Training on collaboration, coordination & alerting and reporting topics & processes seems to be the only training category performed on a monthly basis. Training (of all categories) on a quarterly basis takes place less frequently (<25% per category), while the majority has claimed that training is delivered even less frequently (few times or never).

9.5 Information Sharing (SEs)

Q15. What types of cybersecurity information does your organization regularly share with other entities? (Select all that apply)

Threat Intelligence; Incident alerts & reports; Incident Response & Business Continuity strategies; Best practices and training material; Mandatory reporting; No information sharing

Figure 67: (SEs) Information Sharing Status

The cybersecurity information that is less shared is about Incident Response & Business Continuity strategies, while there is also a small percentage referring to no sharing information at all.

Q16. How does your organization currently collaborate with other critical infrastructure entities and cybersecurity stakeholders? (Select all that apply)

Through formalized partnerships & agreements; Through ad-hoc interactions, as needed; Through interpersonal relationships/communications; Through industry conferences and workshops; Through formally established obligations & processes

Figure 68: (SEs) Collaboration Status

The collaboration with other critical infrastructure entities and cybersecurity stakeholders is achieved mainly through formalized partnerships & agreements and secondarily, through ad-hoc interactions.

Q17. What are the main barriers to more frequent & more effective collaboration, coordination, and overall information sharing with peers and cybersecurity stakeholders, from your perspective? (Common to Q14 (CIOs))

- Lack of standardised processes & protocols
- Data Security & Privacy concerns
- Lack of depth & usability (actionability) of information shared
- Lack of strong relationships & trust between stakeholders
- Legal & Regulatory constraints
- Technical challenges & limitations (e.g., technological capacity, interoperability).

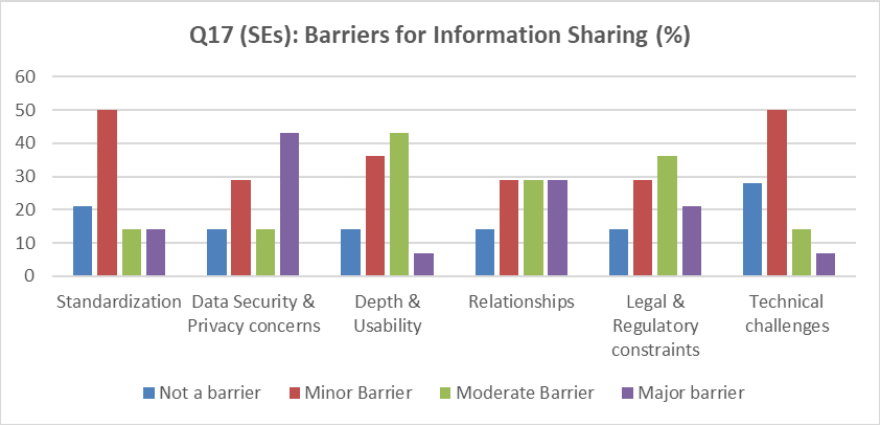


Figure 69: (SEs) Barriers for Information Sharing (%)

- Top cited major barrier seems to be Data Security & Privacy concerns, which indicates hesitation to share due to risks of data breaches or misuse. Lack of strong relationships & trust was also rated as a major (or moderate) barrier. Similarly, Legal & Regulatory constraints were viewed as an important barrier which shows that legal risks significantly impact willingness to share.
- Lack of depth & usability of shared information was flagged as a moderate barrier which highlights a challenge in making shared data actionable or relevant.

- Lack of standardised processes & protocols does not seem to be a critically blocking factor mainly rated as a minor barrier (and secondarily as a major/moderate one), although a need for more uniformity is implied. Similarly, Technical challenges & limitations were noted as a minor barrier or not a barrier, which suggests that technology isn't a key blocker for most respondents.

9.6 Outro (SEs)

Q18. Thinking of the latest cybersecurity regulations enforced or planned to be enforced in the EU (e.g., NIS & NIS2, Cyber Resilience Act), what are the most significant challenges your organisation faces (or will face) to achieve compliance? (Select all that apply; up to 3 selections) (Common to Q15)

- Complexity of regulations
- Frequent changes in regulations
- Lack of internal expertise
- Cost of achieving and maintaining compliance (e.g., cost of investment on relevant capacities)
- Lack of management support (e.g., dedicating enough resources to support compliance)
- Inadequately defined expectations / lack of clarifications (e.g., at the implementation level)

Figure 70: (SEs) Regulation Compliance Challenges

Cost of achieving and maintaining compliance and Complexity of regulations were ranked as the top compliance challenges.

Q19. Overall, moving forward, which of the following aspects would you prioritise (e.g., in terms of investing into new relevant capabilities) in your organisation? (Up to 3 selections) (Common to Q18 (CIOS))

- Security controls (e.g., novel data protection & encryption approaches, access control, host & network controls)
- Local Situational Awareness (e.g., real-time monitoring, threat detection & prioritisation leveraging AI technologies)
- Global Situational Awareness (e.g., access to and contextual understanding of Cyber Threat Intelligence)
- Proactive & Reactive Incident Response (e.g., via Security Orchestration, Automation & Response)

- Business Continuity & Resilience (including Recovery)
- Preparedness (e.g., employee training and awareness)
- Compliance support & validation tools (e.g., certification)

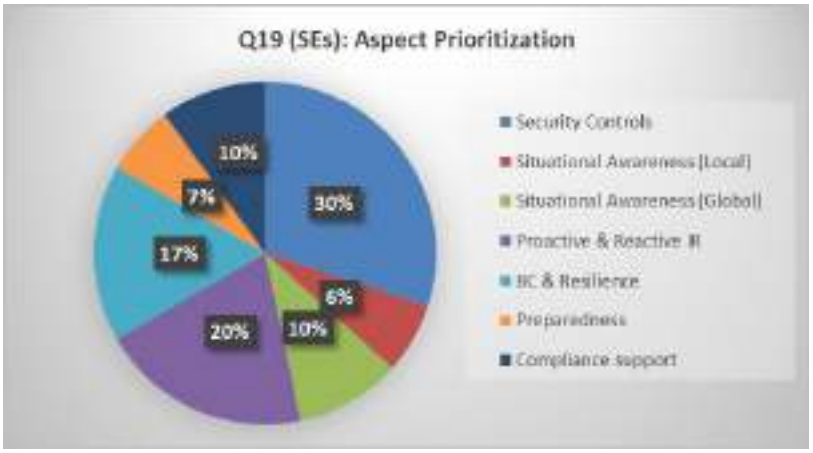


Figure 71: (SEs) Aspect Prioritization

Q20. Having reviewed the provided material regarding the project vision and its outputs, to what extent do you believe PHOENI2X (and similar approaches) could have a positive impact in the following aspects of your organisation's cybersecurity capacity & metrics (Common to Q17 (CIOs))

- Improvement in your business continuity and recovery capacity
- Improvement in your Incident Response processes
- Enhanced alerting and information exchange capacity
- Increase in volume of actionable information received
- Increase in early warnings received
- Increase in proactive actions triggered
- Increase in staff Training & Awareness levels
- Increase in assurance & certification capabilities
- Support in adoption of standardised processes & tools
- Overall increase in coverage of BC, IR and compliance (e.g., NIS/NIS2) requirements

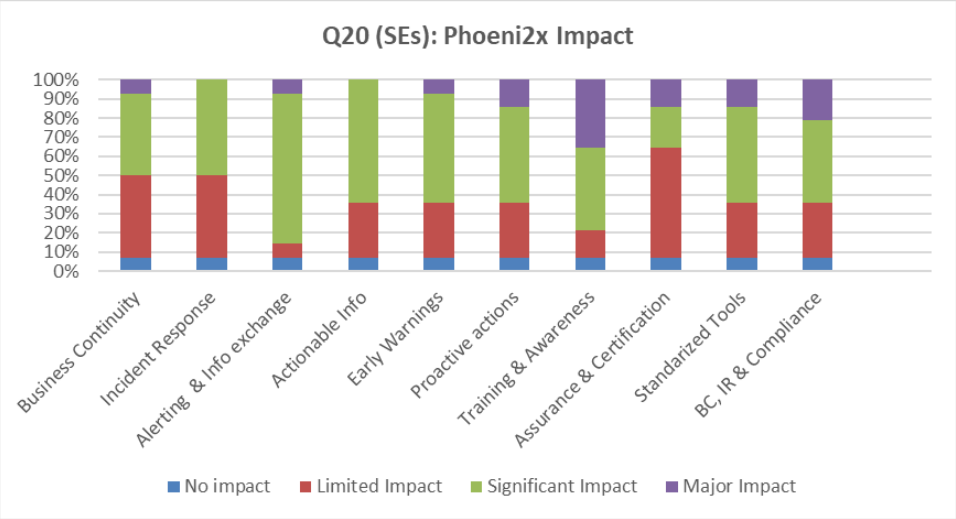


Figure 72: (SEs) PHOENI2X Impact

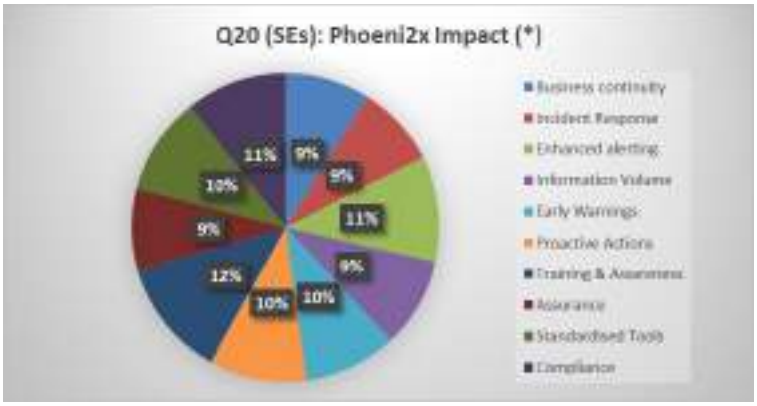


Figure 73: (SEs) PHOENI2X Impact (*)

(*) Used Enumeration: No Impact: 0, Limited Impact: 1, Significant Impact: 2, Major Impact: 3

Almost on all the investigated aspects the PHOENI2X framework is expected to have a major impact. Training and awareness seem to be prioritized.

10 ANNEX - Insights and feedback derived from CIOs

The survey addressing CIOs comprises the following parts:

- Profile/General: Q1 – Q9 10.1
- Situational Awareness: Q10 10.2
- Response (Incident Response & Business Continuity): Q11 10.3
- Preparedness: Q12 10.4
- Information Sharing: Q13 – Q14 10.5
- Outro: Q15 – Q18 10.6

10.1 Profile/General (CIOs)

Q1. Which of the following best describes your organisation?

- Policy Making entities in Cybersecurity
- Critical Infrastructure Organizations/Essential Organizations (under NIS2)
- Important Organizations (as identified by NIS2)
- Security Service Providers / Experts
- IT Companies (not providing security services)
- EU funded projects
- Research organizations
- Other [Transport Company]

Figure 74: Organization Type

The majority of the respondents work for CIOs/OESs.

Q2. Which are the main sectors your organization operates in? (Select all that apply) (Common to Q1 (SEs)

Energy, Telecommunications, Transportation Systems, Healthcare, Information Technology, Financial Services, Policy Making, Other [Cybersecurity]

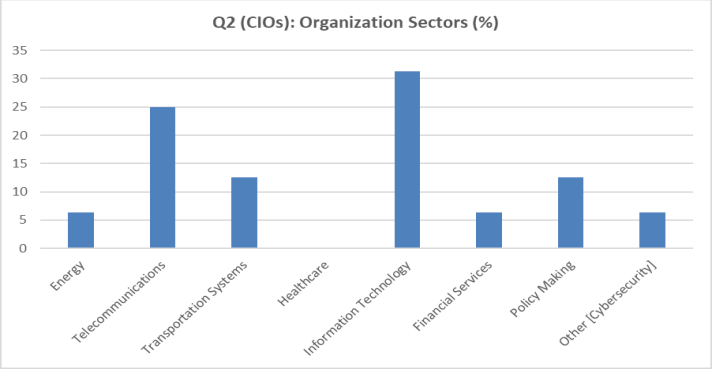


Figure 75: (CIOs) Organization Sectors (%)

Q3. What is your role within your organization? (Common to Q2 (SEs))

CEO/Director; CIO/CTO; CISO; Team Lead/ Manager; IT personnel; Other [Security Advisor]

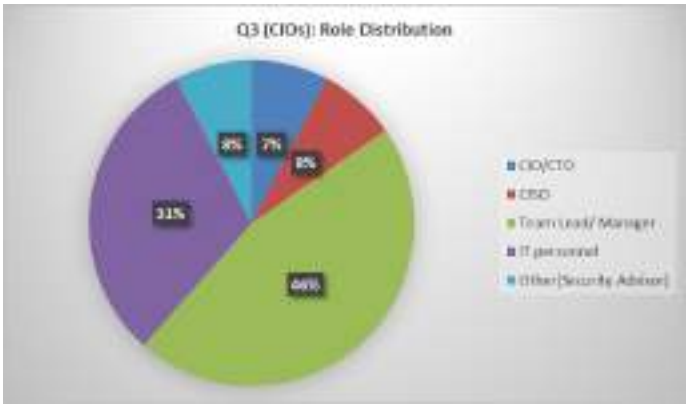


Figure 76: (CIOs) Role Distribution

The majority of the respondents are Managers and secondarily IT personnel.

Q4. Please rank the following concerns in terms of importance, for the protection of critical infrastructures (essential & important services) in the EU? (Rank answers) (COMMON TO Q3 (SEs))

External threats, Internal errors & vulnerabilities, Supply Chain vulnerabilities, Human-related weaknesses, Non-compliance damages, Business Continuity & Client Satisfaction

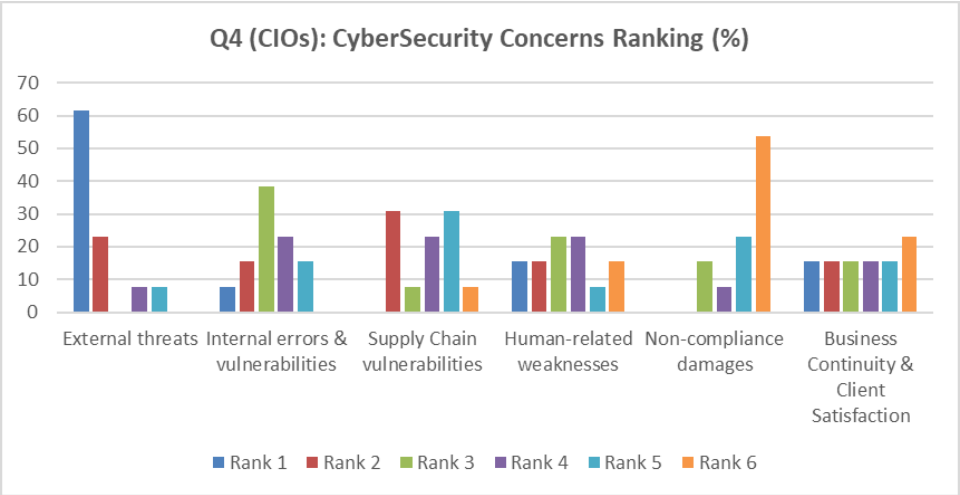


Figure 77: (CIOs) CyberSecurity Concerns Ranking (%)

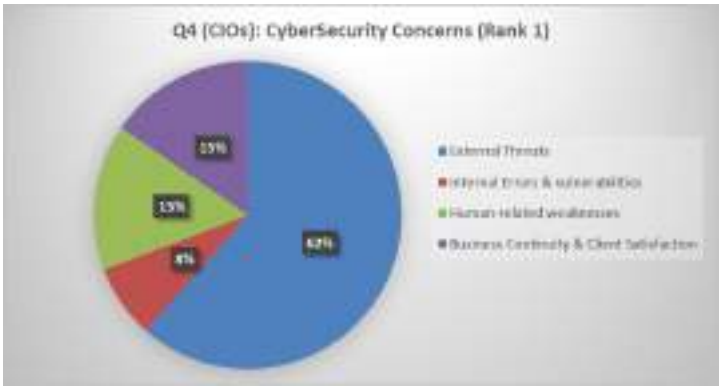


Figure 78: (CIOs) CyberSecurity Concerns (Rank 1)

Rank 1: The majority of participants have selected External threats as the most important issue for protecting critical infrastructures.

Rank 2: Supply Chain vulnerabilities in this rank show concern for unintentional flaws or inherited risks from vendors and partners.

Rank 3: This rank was mostly dominated by Internal errors, Human-related weaknesses, reflecting that many participants see these as relevant but not urgent. In the rest areas (BC, Non-compliance damages) that appear less prominently, it is implied that organizations may already have some controls in place.

Rank 4: Many ranked Supply Chain vulnerabilities, Human-related weaknesses and Non-compliance damages here, suggesting a moderate but not top-of-mind level of concern.

Ranks 5 & 6: Regulatory consequences and third-party risks are perceived as less immediate or tangible; thus not prioritized.

Q5. Please assess each of the below limitations & challenges in terms of the extent that they may hinder your organisation's ability to further improve its cybersecurity posture. (Please select importance of each option: Not an issue/Minor issue/Important issue/Major issue) (Common to Q4 (SEs))

- Difficulty in maintaining situational awareness and visibility in terms of the assets (IT/ OT/ IIoT) in your infrastructure & their status.
- Difficulty in maintaining situational awareness and visibility in terms of pertinent threats that affect you and your peers (threat intelligence)
- Inadequate incident response planning
- Lack of access to relevant cyber-defense tools & technologies
- Difficulty in securing funding to be invested in cybersecurity
- Business continuity planning & implementation
- Translating cybersecurity issues
- Lack of employee training & awareness
- Lack of access to information exchange mechanisms

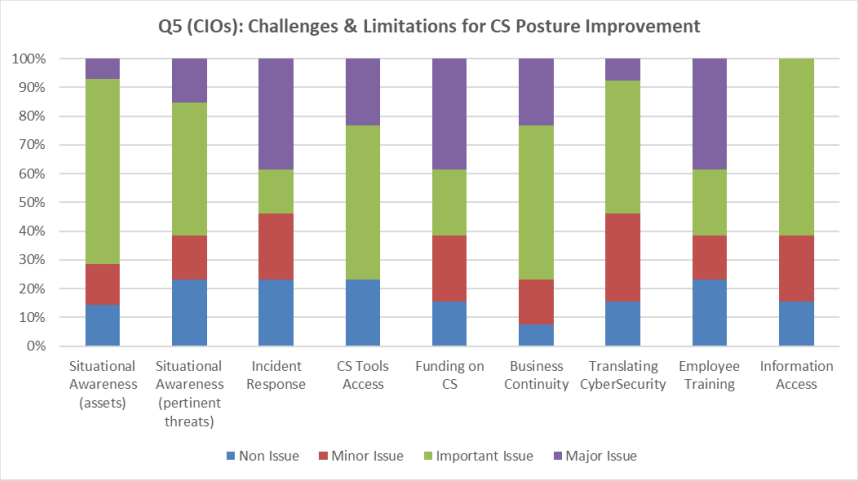


Figure 79: (CIOs) Challenges and Limitations for CS Posture Improvement

- Incident response planning, Funding and Employee training are indicated as top challenges and limitations.
- Access to tools, Situational awareness (both of assets and threats) and Business Continuity remain crucial points for an organization CS posture. Information sharing mechanisms are largely seen as an important gap, which could be addressed through better collaboration and intelligence sharing.

Q6. From a higher level, which would you highlight as the most significant & common barrier in allowing EU organisations to achieve a better cybersecurity posture?

- Technological barriers (e.g., appropriate technologies)
- Organizational barriers (e.g., management priorities, structure)
- Cost barriers (e.g., significant investment required)
- Regulatory barriers (e.g., inadequate or complex regulations)

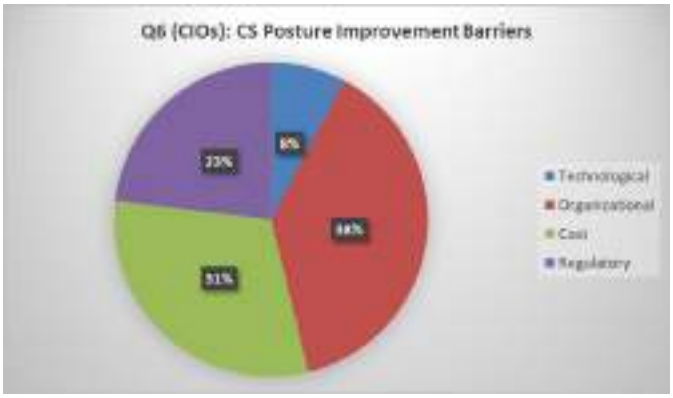


Figure 80: (CIOs) Posture Improvement Barriers

The organizational barriers are cited as most important for a better CS posture, followed by cost issues**.**

Q7. What security frameworks and/or standards would you prioritise as most important to be adopted by EU's organisations as a baseline for their cybersecurity capacity? (Similar to Q5 (SEs))

- NIST Cybersecurity Framework (CSF)
- ENISA/EU Cybersecurity Certification

- ISO27001 family of standards [27001, 27002]
- Industry-specific [DORA, PCI-DSS, HIPAA, GDPR, Internal]

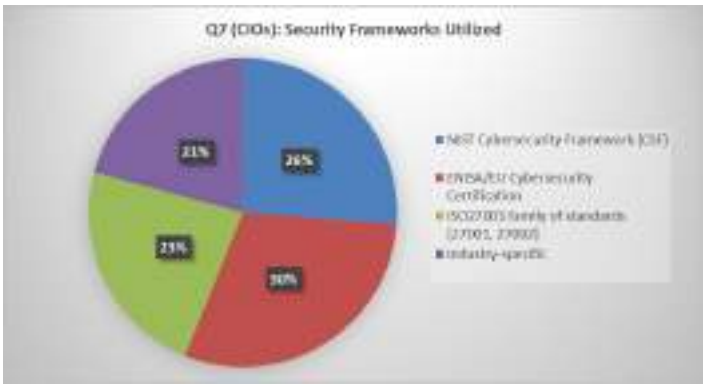


Figure 81: (CIOs) Security Frameworks Utilized

(*) Based on AVG Rank

ENISA/EU Cybersecurity Certification has been prioritized by the CIOs, followed by the NIST CSF.

Q8. Overall, how effective do you consider cybersecurity solutions currently in the market to be in terms of helping organisations achieve resilience against cyber attacks?

Very ineffective; Ineffective**;** Effective**;** Neutral; Very effective

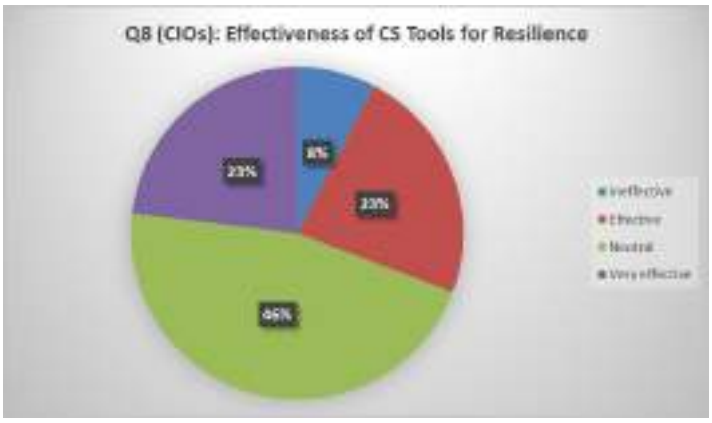


Figure 82: (CIOs) Effectiveness of CS Tools for Resilience

The outcomes indicate that there is room for improvement of the CS tools in terms of resilience.

Q9. Overall, how effective do you consider current cybersecurity solutions to be in terms of helping organisations achieve certifiable compliance with cybersecurity regulations & standards?

Very ineffective; Ineffective; Effective; Neutral; Very effective

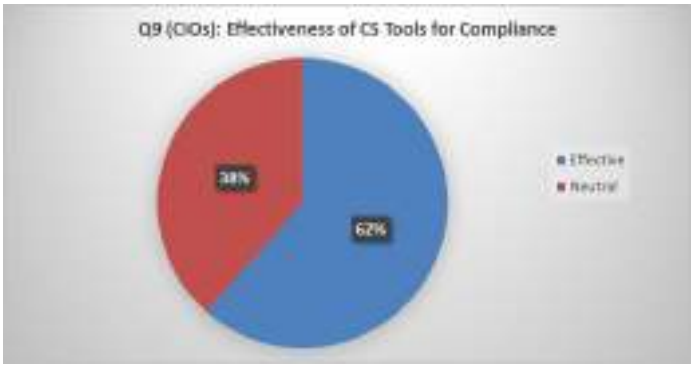


Figure 83: (CIOs) Effectiveness of CS Tools for Compliance

The responses are split between effective and neutral, in favor of the effective selection.

10.2 Situational Awareness (CIOs)

Q10. Which approaches, tools & methods are most important in terms of helping EU's organizations establish better situational awareness regarding cyber threats? (Please rate each option accordingly) (Similar to Q6 (SEs))

Vulnerability Assessments; Penetration Testing; Real-time monitoring of cyber assets; Solutions aggregating security events in real time; Access to timely and relevant CTI information; AI-based tools; Risk-focused impact assessment; Other

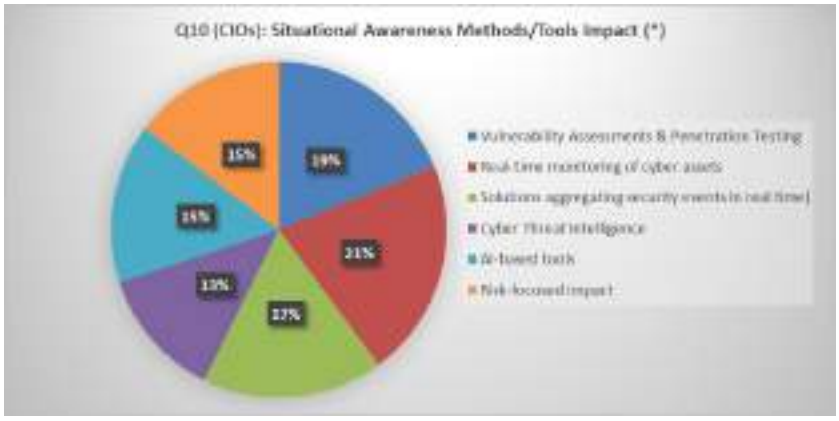


Figure 84: (CIOs) Situational Awareness Methods/Tools Impact (*)

(*)Used Enumeration: Not Important:0, Somewhat Important:1, Important:2, Very Important:3

The three (3) practices mostly affecting Situational Awareness are: Real-time monitoring of cyber assets, Vulnerability Assessments & Penetration Testing and Solutions aggregating security events in real time.

10.3 Response (Incident Response & Business Continuity) (CIOs)

Q11. Rate the following areas in terms of importance for improving your current Incident Response and Business Continuity practices & maturity (Common to Q11 (SEs))

- More effort on identifying critical business functions & maintaining up to date plans
- More comprehensive planning and documentation, including encoding relevant processes in the form of structured workflows (e.g., playbooks)

- Improved access to relevant tools (e.g., for data availability and integrity, monitoring, incident detection)
- Adoption of Automation, Orchestration & Response technologies
- Allocation of more resources (e.g., budget)
- Better communication and coordination during incidents
- Enhanced Training & Awareness programs, including tests & drills, on relevant processes.

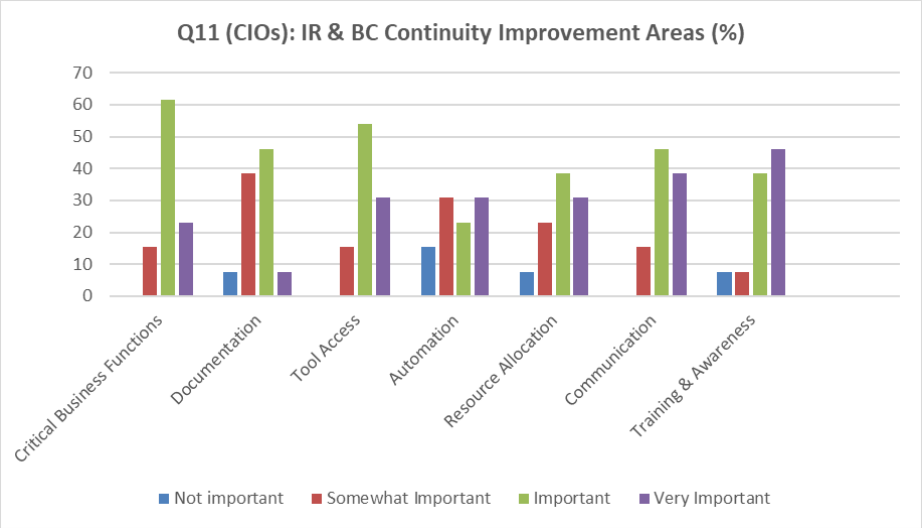


Figure 85: (CIOs) IR and BC Improvement Areas (%)

Figure 86: (CIOs) IR and BC Improvement Areas (*)

(*)Used Enumeration: Not Important:0, Somewhat Important:1, Important:3, Very Important:5

The critical importance of all the areas, especially Training & Awareness programs, Access to relevant tools, better communication during incidents. More effort on critical business functions and Resource allocation are highlighted from the CIOs' responses.

10.4 Preparedness (CIOs)

Q12. Considering the different types of training delivery methods listed below, please rate each based on its potential impact on the training, awareness & overall preparedness of EU organisations to handle cyber threats & incidents. (Similar to Q12 (SEs))

Self-study material provision (e.g., brochures, newsletters, literature); Seminars & Workshops; Interactive Sessions, Tabletop Exercises; Serious Games (e.g., card, online); Realistic, hands-on Training (e.g., Cyber Ranges, Cyber Exercises)

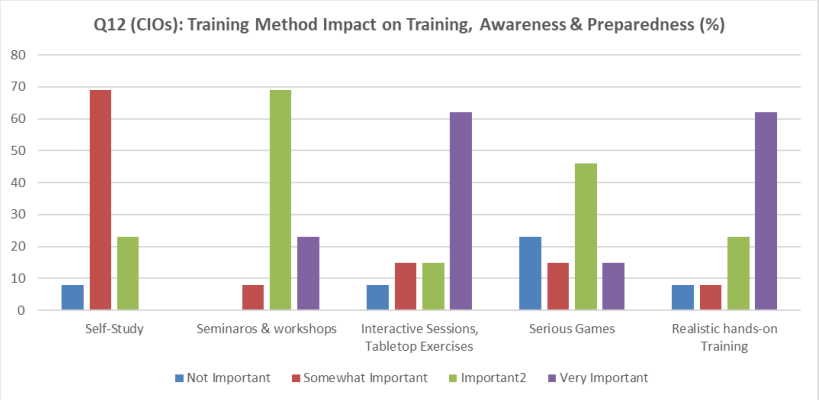


Figure 87: (CIOs) Training Method Impact on Training, Awareness and Preparedness (%)

Figure 88: (CIOs) Training Method Impact on Training, Awareness and Preparedness (*)

(*)Used Enumeration: Not Important: 0, Somewhat Important:1, Important:2, Very Important:3

The most highly valued training methods for awareness and preparedness cited by CIOs are the Realistic hands-on Training, Interactive Sessions & Tabletop Exercises, and Seminars & Workshops.

10.5 Information Sharing (CIOs)

Q13. In terms of providing EU's organisations & other cybersecurity stakeholders with the means and processes for cybersecurity information sharing, what types of information should we prioritise efforts on? (Select up to 3 options)

- Threat Intelligence (technical, operational, etc.);
- Incident alerts & reports
- Incident Response & Business Continuity strategies (e.g., playbooks)
- Best practices and training material (e.g., training content)
- Mandatory reporting (e.g., to relevant National Authorities)

Figure 89: (CIOs) CS Information Sharing Prioritization

The highest priority for information sharing is given to Threat Intelligence (technical, operational, etc.) and Incident alerts & reports.

Q14. What are the main barriers to more frequent & more effective collaboration, coordination, and overall information sharing with peers and cybersecurity stakeholders, from your perspective? (Common to Q17 (SEs))

- Lack of standardised processes & protocols
- Data Security & Privacy concerns
- Lack of depth & usability (actionability) of information shared
- Lack of strong relationships & trust between stakeholders
- Legal & Regulatory constraints
- Technical challenges & limitations (e.g., technological capacity, interoperability).

Figure 90: (CIOs) Barriers for Information Sharing (*)

(*)Used Enumeration: Not a Barrier:0, Minor:1, Moderate:2, Major:3

All the abovementioned barriers are considered as almost equally significant for collaboration and information sharing.

10.6 Outro (CIOs)

Q15. Thinking of the latest cybersecurity regulations enforced or planned to be enforced in the EU (e.g., NIS & NIS2, Cyber Resilience Act), what are the most significant challenges your organisation faces (or will face) to achieve compliance? (Select all that apply; up to 3 selections) (Common to Q18 (SEs))

- Complexity of regulations
- Frequent changes in regulations
- Lack of internal expertise
- Cost of achieving and maintaining compliance (e.g., cost of investment on relevant capacities)
- Lack of management support (e.g., dedicating enough resources to support compliance)
- Inadequately defined expectations / lack of clarifications (e.g., at the implementation level)

Figure 91: (CIOs) Regulation Compliance Challenges

The most significant challenges to achieving cybersecurity compliance in the EU revolve around Lack of internal expertise, Cost issues and Lack of management support.

Q16. Which of the following emerging technologies or trends do you see as having a significant impact on the organizations' cybersecurity posture in the next 2-5 years? (Select all that apply)

- Artificial Intelligence (AI)/Machine Learning (ML)
- Further adoption of Internet of Things (IoT)/Industrial IoT and applications relying on interconnected, smart devices
- Cloud computing & further transition to "as a Service" models
- Increased maturity of Quantum Computing
- Proliferation of tighter cybersecurity regulation

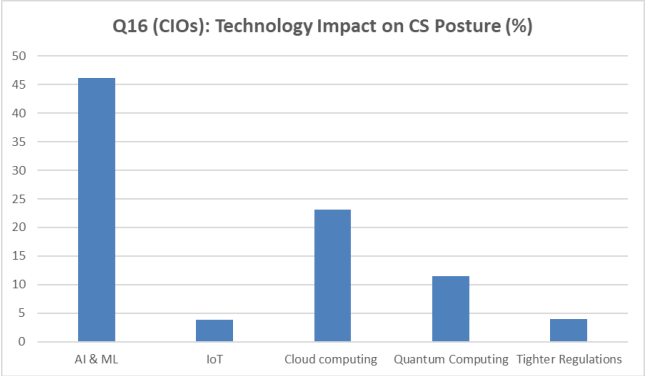


Figure 92: (CIOs) Technology Impact on CS Posture (%)

AI/ML has been rated as the main technology to affect CS posture for the next 2-5 years.

Q17. Having reviewed the provided material regarding the project vision and its outputs, to what extent do you believe PHOENI2X (and similar approaches) could have a positive impact in the following aspects of your organisation's cybersecurity capacity & metrics (Common to Q17 (SEs))

- Improvement in your business continuity and recovery capacity
- Improvement in your Incident Response processes
- Enhanced alerting and information exchange capacity
- Increase in volume of actionable information received
- Increase in early warnings received
- Increase in proactive actions triggered
- Increase in staff Training & Awareness levels
- Increase in assurance & certification capabilities
- Support in adoption of standardised processes & tools
- Overall increase in coverage of BC, IR and compliance (e.g., NIS/NIS2) requirements

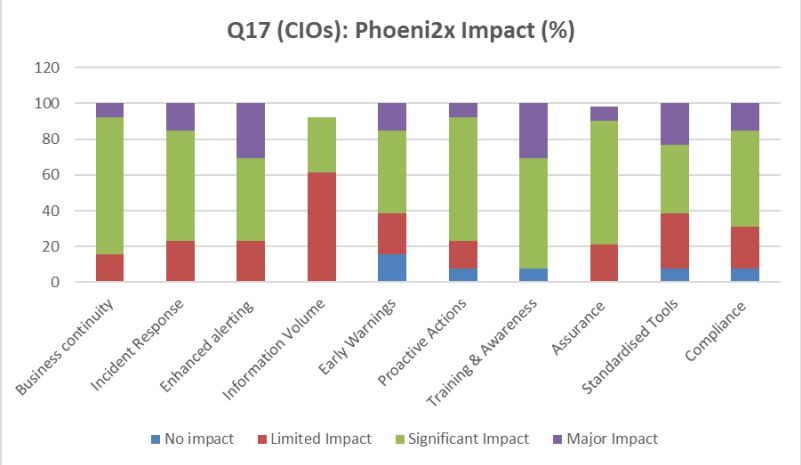


Figure 93: (CIOs) PHOENI2X Impact (%)

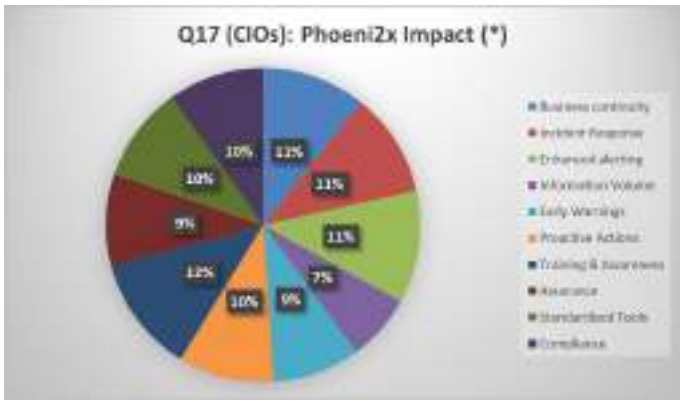


Figure 94: (CIOs) PHOENI2X Impact (*)

(*) Used Enumeration: No Impact: 0, Limited Impact:1, Significant Impact: 2, Major Impact:3

PHOENI2X (and similar frameworks) is generally perceived to have a strong positive impact across multiple areas of cybersecurity capacity, especially in improving business continuity, incident response, training and compliance. While there are areas such as actionable information volume and early warnings that require further focus, overall, respondents see PHOENI2X as a valuable framework for enhancing organizational resilience and response capabilities.

Q18. Overall, moving forward, which of the following aspects would you prioritise (e.g., in terms of investing into new relevant capabilities) in your organisation? (Up to 3 selections) (Common to Q19(SEs))

- Security controls (e.g., novel data protection & encryption approaches, access control, host & network controls)
- Local Situational Awareness (e.g., real-time monitoring, threat detection & prioritisation leveraging AI technologies)
- Global Situational Awareness (e.g., access to and contextual understanding of Cyber Threat Intelligence)
- Proactive & Reactive Incident Response (e.g., via Security Orchestration, Automation & Response)
- Business Continuity & Resilience (including Recovery)
- Preparedness (e.g., employee training and awareness)
- Compliance support & validation tools (e.g., certification)

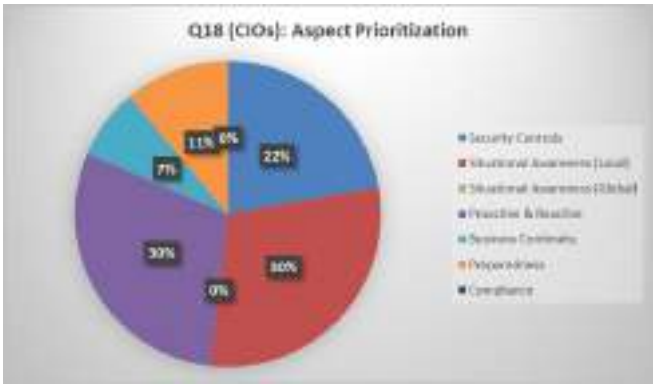


Figure 95: (CIOs) Aspect Prioritization

CIOs clearly prioritize Local Situational Awareness and Proactive & Reactive Incident Response, followed by Security Controls. For Global Situational Awareness and Compliance support has been given no priority.

11 ANNEX – Insights and feedback derived from the interviews

Provided the confidential nature of the interviews**, a summary of the combined insights from all 7 interviews and sectors** (National Authority, Finance, Telecommunications, Naval, Healthcare, Railway and Energy) is provided hereafter, organized by the four common questions.

The interviews reveal shared cybersecurity expectations, sector-specific requirements and strategic implications for service providers.

- **Q1 (INT): What key factors should an organization consider when selecting a cybersecurity service provider?**

Across all sectors, organizations demand that cybersecurity providers demonstrate the following:

Sector-Specific Expertise & Experience: Providers must have deep understanding of operational technologies (OT), data flows, and threat models relevant to each industry. Every sector demands tailored expertise. Indicatively:

Healthcare: PHI and medical devices; Telecom: SS7, GTP, Diameter protocols and 5G infrastructure; Maritime: Securing ECDIS, GPS, AIS, ICS, and satellite communications; Energy: ICS/SCADA protection, regulatory alignment (e.g., NERC CIP); Finance: Compliance (PCI-DSS, SOX), fraud detection, high-value transaction protection; National Authority: National security standards, classified systems, multi-agency coordination; Railway: SCADA & signaling systems.

Cyber Maturity & Resilience: Providers must adhere to the same security standards they recommend — Zero Trust Architecture, 24/7 SOC, threat intel integration, and compliance certifications (ISO 27001, IEC 62443, etc.)

Regulatory Alignment: Familiarity with and proactive compliance across NIS 2, GDPR, HIPAA, IMO, 3GPP, and sector-specific mandates is considered essential.

Reputation & Reliability: Providers are expected to bring demonstrated trustworthiness and integrity, especially in high-risk environments (e.g., hospitals, government systems).

Business Continuity and Viability: Long-term financial and operational stability is critical to avoid supply chain disruption, particularly in critical infrastructure sectors (e.g., energy grid, telecom, hospitals).

Comprehensive and Scalable Services: Providers should offer full-spectrum services (threat detection, incident response, vulnerability management, compliance). In addition, solutions must scale with organizational growth and changing needs.

- **Q2 (INT): How do you ensure services stay current with evolving cyber threats and compliance requirements?**

Key Strategies mentioned:

Real-Time Threat Intelligence: All sectors rely on continuous threat feeds (Sources: MITRE ATT&CK, GSMA T-ISAC, ENISA, ISACs, OSINT as well as AI-based anomaly detection is increasingly standard). In addition, integration with sector-specific platforms (e.g., FS-ISAC, GSMA T-ISAC, ENISA, Maritime ISAC) ensures rapid detection of new threats.

Proactive & Reactive Strategy: Including blend of proactive threat hunting and reactive incident response and lessons from real-world breaches feed into future service updates.

Regulatory Monitoring & Adaptation: Dedicated compliance teams track evolving laws (NIS2 Directive, GDPR, HIPAA, IMO MSC.428, PCI-DSS, 3GPP, etc.) and services are continuously updated to align with new requirements.

Continuous Skills Development: Investment in upskilling, simulations and Certification (e.g., CISSP, CEH, ISO 27001), participation in conference and simulation exercises and sector-specific training (e.g.,

GPS spoofing drills in maritime, red teaming in finance) to stay current with tactics, tools and sector-specific developments.

AI-Driven Monitoring & Analytics: Adoption of AI/ML and anomaly detection is becoming standard for Telecom, Maritime and Energy providers.

Active Sector Participation: Participation in forums, workshops, working groups and other training programs/sessions to influence and align with industry standards.

- **Q3 (INT): How are cybersecurity services customized for sector-specific needs?**

Sector-Specific Threat Modeling & Risk Assessment: Each industry has unique threat actors and attack surfaces and expects tailored solutions built on domain knowledge and operational alignment. Indicatively:

Railway: Protection of safety-critical OT (signaling, SCADA), real-time monitoring of rolling stock, and integration with public infrastructure defenses; Healthcare: Ransomware resilience, PHI protection, and compliance with medical device regulations and continuity of care imperatives; Telecom: Deep protocol-level expertise (GTP, SS7), 5G/MEC security, and DDoS defense. Emphasis on sovereign data controls and lawful intercept compliance; Maritime: Protection of shipboard systems (ECDIS, AIS, GPS), secure ship-to-shore links, and port terminal cybersecurity aligned with IMO and ISO standards; Financial: Transaction security, fraud prevention, regulatory compliance (AML, PSD2), and resilience of customer-facing systems; Energy: ICS/SCADA segmentation, substation protection, and alignment with critical infrastructure protection guidelines; National Authority: Insider threat detection, classified data protection, and secure cloud adoption at national scale.

Tailored Compliance Frameworks: Mapping to sector-specific standards (e.g., IEC 62443 for ICS, IMO guidelines for maritime, PCI-DSS for finance).

Customized Security Architecture: Zero Trust for tech, port and telecom networks; Secure ship-to-shore comms (encrypted SATCOM, LTE-M) for maritime; Endpoint security for healthcare and remote workers; AI-based defense tools in fast-paced tech environments.

Organizational and Cultural Integration: Board-level alignment and risk appetite assessment, as well as industry-specific awareness programs (e.g., finance employees trained to spot wire fraud; medical staff on phishing prevention).

- **Q4 (INT): How is the success or effectiveness of delivered security services assessed?**

Indicative measures mentioned:

Response Metrics: MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), Number of incidents mitigated or contained

Compliance Health: Reduction in audit findings, Real-time tracking of regulatory alignment

User Behavior Indicators: Phishing simulation results, Training effectiveness and security culture metrics

Vulnerability Management: Speed and completeness of patching; Resolution of critical system exposures

Strategic Reporting: Board-level dashboards, Lessons learned and continuous improvement tracking.