Harmonizing People, Processes, and Technology for Robust Cybersecurity

D1.3 Annual report on KPIs assessment v1

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.CYberSynchrony.eu/		
Deliverable	D1.3 Annual report on KPIs assessment v1		
Work Package	WP1 Project Management		
Contractual due date	31.05.2025	**Actual submission date**	11.06.2025
Type	Report	**Dissemination Level**	Public
Lead Beneficiary	MAG		
Responsible Author	Violeta Vasileva (MAG)		
Contributions from	Alexandros Psychas (MAG), Panayiotis Klitou (EBOS)		

Funded by the European Union

ECCC

Funded by the European Union under Grant Agreement no. 101158555 and supported by the European Cybersecurity Competence Centre (ECCC). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	28.04.2025	Initial Deliverable structure	Violeta Vasileva (MAG)
0.2	22.05.2025	Final draft ready for internal review	Violeta Vasileva (MAG)
0.3	23.05.2025	Input by eBOS and MAG	Panayiotis Klitou (EBOS), Alexandros Psychas (MAG)
0.4	26.05.2025	Peer review	Evangelos Michos (IANUS)
0.5	28.05.2025	Peer review	Platon Rizopoulos (EGL)
0.6	29.05.2025	Peer review	Athina Skarpeti (AMC)
0.7	30.05.2025	Final draft addressing comments from internal review	Violeta Vasileva (MAG)
0.8	05.06.2025	Final quality check	Panayiotis Klitou (EBOS)
1.0	11.06.2025	Final version ready for submission	Violeta Vasileva (MAG)

Disclaimer

The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

1 Executive Summary 6
2 Introduction 7
2.1 Mapping CYberSynchrony Outputs 7
2.2 Linkage to other project outputs 7
2.3 Deliverable Structure 8
3 Project Objectives and Related KPIs 10
3.1 Objective 1 10
3.2 Objective 2 11
3.3 Objective 3 12
3.4 Objective 4 14
3.5 Objective 5 16
3.6 Objective 6 17
3.7 Objective 7 18
3.8 Objective 8 18
3.9 Objective 9 19
4 Use Case KPIs 21
4.1 Overview of Use Cases 21
4.2 KPIs per Use Case 23
5 Key Exploitable Results (KERs) 26
6 KPI Dashboard Summary 28
7 Deviations and Mitigation Measures 33
7.1 Potential or Anticipated Deviations 33
7.2 Mitigation Measures 33
8 Conclusions 34
9 References 35

List of Tables

Table 1: Adherence to CYberSynchrony's GA 7
Table 2: Links to other Project Outputs/Work 7
Table 3: Objective 1 KPIs 10
Table 4: Objective 2 KPIs 11
Table 5: Objective 3 KPIs 12
Table 6: Objective 4 KPIs 14
Table 7: Objective 5 KPIs 16
Table 8: Objective 6 KPIs 17
Table 9: Objective 7 KPIs 18
Table 10: Objective 8 KPIs 19
Table 11: Objective 9 KPIs 19
Table 12: Use Case KPIs 23
Table 13: Key Exploitable Results (KERs) 26

© CYberSynchrony, 2024

Table 14: KPI Dashboard Summary 28
Table 15: Communication KPIs, targets and status 31
Table 16: Dissemination KPIs, targets, and status 32

© CYberSynchrony, 2024

Acronyms and abbreviations

Abbreviation / Term	Description
AI	Artificial Intelligence
CISO	Chief Information Security Officer
CYBERA	Cyber Analytics and Risk Assessment Module
CYBERGOPLUS	Compliance and Governance Framework Module
CYBERWISE	Cybersecurity Awareness and Training Platform
CYBRITE	Cyber Response and Incident Tracking Environment
CROSS-CORE	Secure Data Exchange and Coordination Platform
CYRESCUE	Penetration Testing and Incident Simulation Toolkit
D&C	Dissemination and Communication
DORA	Digital Operational Resilience Act
ECCC	European Cybersecurity Competence Centre
EHR/EMR	Electronic Health Records / Electronic Medical Records
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoMT	Internet of Medical Things
IPR	Intellectual Property Rights
IT	Information Technology
KPI	Key Performance Indicator
KER	Key Exploitable Result
MISP	Malware Information Sharing Platform
MOS	Mean Opinion Score (used for usability ratings)
MS	Member States
NIS2	Network and Information Security Directive 2
OA	Open Access
PEN Test	Penetration Test
PII	Personally Identifiable Information
SOAR	Security Orchestration, Automation and Response
SIEM	Security Information and Event Management
STIX/TAXII	Structured Threat Information Expression / Trusted Automated Exchange of Intelligence Information
TTPs	Tactics, Techniques, and Procedures
UPRC	University of Piraeus Research Center
WP	Work Package

© CYberSynchrony, 2024

1 Executive Summary

In its first year of implementation, the **CYberSynchrony project** has focused on laying a solid foundation for achieving its long-term objectives. Core efforts have been directed at setting up governance structures, refining work package interlinkages, developing technical baselines and initiating the technical correlation of critical modules such as CYRESCUE, CYBERRA, CYBRITE, CROSS-CORE and CYBERWISE. Rather than immediate results, the first year has prioritized strategic alignment, stakeholder coordination, and preparatory actions to support impactful KPI delivery in subsequent phases.

Significant progress has been made in establishing a **comprehensive KPI tracking framework** aligned with the project's 9 strategic objectives and 3 use case domains (healthcare, public administration, and higher education). All Key Performance Indicators (KPIs) have been fully defined with clear methodologies, targets and associated validation deliverables. A central KPI dashboard structure has been designed and embedded into the quality assurance process to enable consistent monitoring, benchmarking, and early detection of deviations.

The project has also:

- Mapped each KPI to its respective technological module, work package objective, and verification deliverable.
- Designed data collection processes and analytics protocols for platform usability, threat detection efficiency, user satisfaction and security remediation time.
- Initiated baseline assessments for use case environments to establish pre-implementation benchmarks.

While no quantitative KPI outcomes are available yet, early observations from the tracking framework have surfaced important **risks and opportunities**:

- **Risks**: Potential delays in real-world data acquisition due to the complexity of integrating pilots across diverse sectors (e.g., public health, academia). Additionally, harmonizing measurement standards across Member States may present challenges.
- **Opportunities**: The modular architecture and rigorous tracking design offer high scalability and adaptability. Early coordination among partners has fostered a shared understanding of KPI expectations, enabling proactive mitigation planning.

The CYberSynchrony consortium remains committed to a methodical, quality-driven implementation process. The first year has successfully positioned the project to transition into measurable implementation and evaluation phases into Year 2.

© CYberSynchrony, 2024

2 Introduction

2.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony's Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, in respect to their outputs and work to be performed.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D1.3	Annual Report on KPIs Assessment	Chapters 3–8	Provides a comprehensive review of all KPIs, linking them to project objectives and use cases. Lays the groundwork for future KPI measurement and outlines methodology, deviations, and mitigation strategies.
TASKS			
Task number T1.3	KPI Monitoring and Reporting Framework	Chapters 3, 4, 6, 7	Establishes the full list of KPIs, defines tracking mechanisms, links to modules and use cases, and sets up a dashboard for future monitoring. Includes methodologies, baseline setting, and early deviations.

2.2 Linkage to other project outputs

The table below explains how the deliverable is related to other project outputs and specific deliverables.

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP1	T1.1, T1.3	D1.1	D1.3 (this report) builds directly on D1.1 by defining, aligning, and structuring the KPI tracking and reporting system.

© CYberSynchrony, 2024

WP2	T2.1, T2.2	D2.1	Technical inputs for threat intelligence and risk assessment KPIs under Objectives 1 and 3. These support early benchmarking and system capability metrics.
WP3	T3.1, T3.2	D3.1, D3.2	Informs KPIs on AI-driven threat detection and platform performance for Objectives 1 and 7.
WP4	T4.1, T4.2	D4.1, D4.2	Core input for incident detection and response KPIs tied to Objectives 2, 3, and 7.
WP5	T5.1, T5.2	D5.1, D5.2	Related to secure communication KPIs and effectiveness of risk monitoring tools for Objective 5.
WP8	T8.1, T8.2, T8.3, T8.4	D8.1	Cross-border exercises and simulation data feeding into KPIs for Objective 4.
WP9	T9.1, T9.2, T9.3, T9.4	D9.1, D9.2	Exploitation and commercialization strategy linked to Objective 9 KPIs, especially regarding KERs, stakeholder engagement and adoption of best practices.

2.3 Deliverable Structure

This deliverable is structured to provide a clear and systematic overview of the KPI framework designed for the CYberSynchrony project. It outlines the methodological foundation, the initial alignment of KPIs with project objectives, and the setup of tracking mechanisms for ongoing monitoring and evaluation. The structure of the document is as follows:

- **Chapter 1: Executive Summary**

  Presents a concise overview of the project's first-year progress, the current status of KPI implementation, and the emerging risks and opportunities observed through the initial monitoring setup.

- **Chapter 2: Introduction**

  Defines the purpose, scope, and relevance of the deliverable. It also provides the mapping of the deliverable to the Grant Agreement, highlights its relationship with other project outputs, and introduces the structural composition of the document.

- **Chapter 3: Project Objectives and Related KPIs**

  Details each of the nine project objectives and the corresponding Key Performance Indicators (KPIs), including definitions, targets, and measurement methodologies.

- **Chapter 4: Use Case KPIs**

© CYberSynchrony, 2024

Introduces the three pilot use cases (healthcare, public administration, and higher education) and outlines the KPIs tailored to each environment, supporting applied validation of the core objectives.

- **Chapter 5: Key Exploitable Results (KERs)**

Summarizes the preliminary list of exploitable outputs and their potential relevance to KPI measurement, with links to future exploitation deliverables.

- **Chapter 6: KPI Dashboard Summary**

Provides a high-level summary table that consolidates all KPI targets, linked objectives, and their current status (where applicable), establishing the foundation for future progress tracking.

- **Chapter 7: Deviations and Mitigation Measures**

Identifies any anticipated or emerging risks in meeting KPI targets, outlines reasons for potential deviations, and proposes mitigation strategies for realignment.

- **Chapter 8: Conclusions**

Concludes the deliverable by summarizing the key contributions of the KPI framework to the overall project strategy and providing insights into how these efforts will evolve in the following project phases.

© CYberSynchrony, 2024

3 Project Objectives and Related KPIs

At this stage, aside from the D&C KPIs, no measurable progress has been made. The current version and the related deliverables mentioned in the verification section, mainly outlines the methodology and how each KPI will be addressed during implementation.

3.1 Objective 1

Enhance the threat assessment and risk monitoring services, enabling quicker identification of threats and attacks by leveraging state-of-the-art threat intelligence platform (e.g. MISP, STIX/TAXI, ThreatConnect) and attackers' profiles models that utilizes artificial intelligence to gather and analyse real-time information about emerging cyber threats and attackers' behaviour.

Related modules: CYRESCUE, CYBERRA, CYBRITE

Verification: D2.1, D2.2, D3.1, D3.2.

Table 3: Objective 1 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI1.1	Number of Threat Assessments Carried Out	Measure the quantity of threat assessments conducted using the state-of-the-art threat intelligence platform gathering real-time information about emerging cyber threats and attack potential, analysing their potential impact and vulnerability severity, on critical infrastructure, essential entities, and digital services aiming to improve the threat assessment capabilities and enhance the early detection and response to potential cyber threats	>36 threat assessments aiming to enhance the platforms' capabilities to identify and respond to emerging cyber threats promptly.	
KPI1.2	Number of Risk Scenario Analyses Carried Out	Track the number of risk scenario analyses performed using the advanced threat intelligence platform to understand the risks to develop effective strategies for risk management and incident response.	Perform at least 13 risk assessments aiming to improve risk assessment capabilities and enable more effective risk management and incident response strategies.	
KPI1.3	Threat Intelligence platform effectiveness	Measure the platform's ability to detect and mitigate threats successfully.	Achieve a threat detection and mitigation rate > 85%, indicating that out of every 100 potential	Regularly test the platform with simulated threats and real-world data.

© CYberSynchrony, 2024

			threats, the platform can successfully identify and neutralize 85 of them within the specified timeframe.	
KPI1.4	Threat Intelligence platform Usability	User Satisfaction Rating measures the satisfaction level of users, such as security analysts and incident responders, with the platform's usability and features	Increase the user satisfaction rating to 4.5 out of 5 MOS aiming to enhance the usability and provide a more intuitive user experience.	
KPI1.5	Threat Intelligence platform Security	Platform Vulnerability Remediation Time measures the time taken to identify and remediate vulnerabilities in the Threat Intelligence platform	Reduce the platform vulnerability remediation time to 15 days aiming for faster remediation of vulnerabilities enhancing the platform's security posture.	
KPI1.6	Threat Intelligence platform Security Incident Response Time	Measures the time taken to respond to and address security incidents with particular emphasis on zero-day threats, within the Threat Intelligence platform.	Reduce the security incident response time for zero-day threats to 4 hours and for other threats to 8 hours in the current year compared to last year, ensuring expedited containment and mitigation of incidents.	

3.2 Objective 2

Minimize the duration and impact of cyber incidents with timely and coordinated incident response by integrating automation and orchestration capabilities in incident response coordination tools by automating repetitive tasks and orchestrating incident response workflows, the efficiency of response efforts can be significantly increased, leading to faster containment and mitigation of cyber incidents enabling faster and more effective response efforts.

Related modules: CROSS-CORE,

Verification: D4.2

Table 4: Objective 2 KPIs

KPI ID	Name	Description	Target	Measurement Methodology

© CYberSynchrony, 2024

KPI2.1	Number of Penetration Tests Provided	Measure the quantity of penetration tests provided to assess the security of systems, networks, and applications simulating real-world cyberattacks to identify vulnerabilities and weaknesses that could be exploited by malicious actors.	>= 60 penetration tests.	
KPI2.2	Incident Detection Time	Measure the average time taken to detect and identify cyber incidents, including the initial breach or suspicious activity.	Reduce the average incident detection time to 3 days.	
KPI2.3	Incident Response Time	Track the average time taken to respond and initiate incident response actions after the detection of a cyber incident	Reduce the average incident response time to 15 days.	
KPI2.4	Incident Resolution Rate	Measure the percentage of cyber incidents successfully resolved and mitigated without further impact.	Achieve at least an 80% incident resolution rate within 24 hours compared to last years	Track the time and outcomes of incident responses.

3.3 Objective 3

Strengthen the risk monitoring services and early detection of cyber incidents by deploying advanced cybersecurity analytics tools to analyse network traffic, software security, user behaviour, and system activity identifying anomalous activities and insider threats.

Related modules: CYBERRA, CYBRITE

Verification: D4.1.

Table 5: Objective 3 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI3.1	Number of Threat Assessments Carried Out	Measure the quantity of threat assessments conducted using the state-of-the-art threat intelligence platform gathering real-time information about emerging cyber threats, analysing their potential impact on critical infrastructure, essential entities, and	Conduct at least 36 threat assessments aiming to enhance the platforms' capabilities to identify and respond to emerging cyber threats promptly	

© CYberSynchrony, 2024

		digital services. Aim: Improve the threat assessment capabilities and enhance the early detection and response to potential cyber threats.		
KPI3.2	Number of Risk Scenario Analyses Carried Out	Track the number of risk scenario analyses performed using the advanced threat intelligence platform to understand the risks in order to develop effective strategies for risk management and incident response.	Perform at least 13 risk scenario analyses aiming to improve risk assessment capabilities and enable more effective risk management and incident response strategies.	
KPI3.3	Number of Potential Users Covered per Test/Exercise	Measure the coverage of potential users, such as employees, in cybersecurity tests and exercises assessing the organization's readiness to respond to cyber incidents and ensure that relevant personnel are well-prepared to handle potential threats.	Increase the coverage to an average of 150 potential users per test/exercise	
KPI3.4	Number and Nature of Vulnerabilities Discovered	Track the number of vulnerabilities discovered using advanced cybersecurity analytics tools during various assessments, including threat assessments and risk scenario analyses evaluating the severity and criticality of the vulnerabilities to prioritize remediation efforts.	Reduce the number of high-severity vulnerabilities by 15% compared to other approaches while maintaining the overall discovery rate aiming to identify and address high-severity vulnerabilities more effectively without compromising the overall discovery efforts	Use vulnerability scanning tools and manual assessments and compare findings with previous assessments and benchmark against industry averages
KPI3.5	Threat Intelligence platform Security	Platform Vulnerability Remediation Time measures the time taken to identify and remediate vulnerabilities in the Threat Intelligence platform.	Reduce the platform vulnerability remediation time to 15 days aiming for faster remediation of vulnerabilities enhancing the	

© CYberSynchrony, 2024

			platform's security posture.	
KPI3.6	Risk Scenarios Analysed	Track the number of customized risk scenarios analysed to assess the impact of potential cyber threats on critical sectors and systems.	Increase the number of analysed risk scenarios by 15% aiming to analyse at least 12 customized risk scenarios to improve risk assessment capabilities.	Review each scenario analysis and compare year over- year changes in the number and complexity of scenarios.
KPI3.7	Risk Mitigation Index	Measure the effectiveness of risk mitigation strategies based on the reduction of identified risks.	Achieve a 20% reduction in identified risks through more effective risk mitigation strategies aiming to improve the risk mitigation index and achieve better risk management outcomes.	Quantify risks before and after mitigation strategies are implemented, risk assessment frameworks could be used for consistent measurement.

3.4 Objective 4

Enhance mutual assistance among MS and facilitate more frequent and realistic cross-border cyber exercises and behavioural change interventions by leveraging virtual cyber range platforms to simulate complex cyber scenarios across borders, critical infrastructure, and digital services enabling more realistic and frequent joint cybersecurity exercises, to bolster mutual assistance efforts and ensure better preparedness for large-scale cross-border cyber incidents.

Related modules: CYRESCUE, CROSS-CORE

Verification: D8.1, D8.2

Table 6: Objective 4 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI4.1	Number of Penetration Tests Provided.	Number of Penetration Tests Provided. Measure the quantity of penetration tests provided to assess the security of systems, networks, and applications simulating real-world cyberattacks	60 penetration tests planned, representing a 20% increase in frequency, to further validate the	

© CYberSynchrony, 2024

		to identify vulnerabilities and weaknesses that could be exploited by malicious actors.	robustness of the system's security, by reducing successful penetrations to 0. The goal is to achieve a 0% success rate for attackers by ensuring that each additional penetration attempt is successfully deterred.	
KPI4.2	Number of Cross-Border Actions/Exercises	Quantify the number of cross-border actions and joint cybersecurity exercises facilitated by the virtual cyber range platforms involving collaborative efforts between different MS to address cyber incidents or conduct joint cybersecurity exercises.	10 cross-border actions/exercises aiming	
KPI4.3	Vulnerabilities Addressed	Track the number of identified vulnerabilities that have been addressed and remediated by critical infrastructure operators and digital service providers	Address and remediate at least 80 vulnerabilities.	
KPI4.4	Number and nature of Vulnerabilities Discovered	Track the number of vulnerabilities discovered using advanced cybersecurity analytics tools during various assessments, including threat assessments and risk scenario analyses evaluating the severity and criticality of the vulnerabilities to prioritize remediation efforts	Reduce the number of high-severity vulnerabilities by 15% compared to other approaches	Use vulnerability scanning tools and manual assessments and compare findings with previous assessments and benchmark against industry averages.
KPI4.5	Incident Collaboration Index	Measure the effectiveness of cross-border incident response coordination based on successful collaborative efforts	Increase the Incident Collaboration Index to 70%	Track and analyse cross-border incident response collaborations. Survey participants for effectiveness

© CYberSynchrony, 2024

				and areas of improvement

3.5 Objective 5

Ensure data privacy and security during information exchange by establishing a secure and standardized communication infrastructure for sharing incident data, threat intelligence, and best practices among MS and relevant stakeholders utilizing encrypted communication channels.

Related modules: CYRESCUE, CROSS-CORE

Verification: D5.1, D5.2.

Table 7: Objective 5 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI5.1	Number of Risk Monitoring Services Provided	Measure the quantity of risk monitoring services that are offered as part of the secure communication and information sharing infrastructure involving the continuous and proactive surveillance of critical systems, networks, and data to detect potential cyber threats and vulnerabilities	Activate 25 risk monitoring services, while at least 95% of them should achieve a user satisfaction rating of 4 out of 5, based on criteria such as accuracy of threat detection, timeliness of alerts, and comprehensiveness of monitoring coverage. Additionally, they should maintain false positive rate of < 5%, ensuring that the vast majority of alerts generated are relevant and actionable	Conduct user surveys to assess satisfaction and effectiveness
KPI5.2	Information Sharing Frequency	Measure the frequency of information sharing among MS during cyber incidents and crises	Increase the information sharing frequency to 75% of cyber incidents and crises	Track information-sharing instances and compare them to the total number of incidents

© CYberSynchrony, 2024

3.6 Objective 6

Foster greater collaboration and knowledge sharing among stakeholders in the cybersecurity ecosystem utilizing advanced technologies by enabling real-time information exchange and joint exercises, aiming the MS to learn from each other's experiences and collectively improve their cybersecurity capabilities.

Related modules: CYRESCUE, CYBERRA, CROSS-CORE

Verification: D6.1, D6.2.

Table 8: Objective 6 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI6.1	Number of Penetration Tests Provided	Measure the quantity of penetration tests provided to assess the security of systems, networks, and applications simulating real-world cyberattacks to identify vulnerabilities and weaknesses that could be exploited by malicious actors.	60 penetration tests planned — a 20% increase to strengthen security and achieve a 0% attacker success rate, ensuring all attempts are effectively blocked.	
KPI6.2	Number of Threat Assessments Carried Out	Track the number of threat assessments conducted using a real-time threat intelligence platform to enhance early detection and response for critical infrastructure and digital services.	> = 36 threat assessments	
KPI6.3	Number of Risk Scenario Analyses Carried Out:	Track the number of risk scenario analyses performed using the advanced threat intelligence platform to understand the risks to develop effective strategies for risk management and incident response.	>= 13 risk scenario analyses	
KPI6.4	Vulnerabilities Addressed	Track the number of identified vulnerabilities that have been addressed and remediated by critical infrastructure operators and digital service providers.	>= 80 vulnerabilities	

© CYberSynchrony, 2024

KPI6.5	Threat Intelligence platform Security	Platform Vulnerability Remediation Time measures the time taken to identify and remediate vulnerabilities in the Threat Intelligence platform	Reduce remediation Time to 15 days	

3.7 Objective 7

Enhance early detection and response to cyber incidents by leveraging Advanced threat intelligence and analytics while reducing the impact of potential cyber threats on critical infrastructure and essential entities.

Related modules: CYBERRA, CYBRITE, CROSS-CORE

Verification: D3.1, D3.2, D4.1

Table 9: Objective 7 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI7.1	Number and Nature of Vulnerabilities Discovered	Track the number of vulnerabilities discovered using advanced cybersecurity analytics tools during various assessments, including threat assessments and risk scenario analyses evaluating the severity and criticality of the vulnerabilities to prioritize remediation efforts.	Reduce by 15% compared to other approaches	Use vulnerability scanning tools and manual assessments and compare findings with previous assessments and benchmark against industry averages
KPI7.2	Vulnerabilities Addressed	Track the number of identified vulnerabilities that have been addressed and remediated by critical infrastructure operators and digital service providers	>= 80 vulnerabilities	

3.8 Objective 8

Implement cybersecurity awareness campaigns and educational programs targeting citizens, businesses, and organizations while fostering a culture of cybersecurity awareness and best practices across all levels of society.

Related module: CYBERWISE

Verification: D6.1, D6.2

© CYberSynchrony, 2024

Table 10: Objective 8 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI8.1	Cybersecurity Training Coverage	Measure the percentage of citizens, businesses, and organizations that have undergone cybersecurity training and awareness programs.	Increase cybersecurity training coverage to 85%	Track participation in training programs and assess the effectiveness of the training through surveys and tests.
KPI8.2	Cybersecurity Awareness Index	Measure the level of cybersecurity awareness among citizens and organizations based on surveys and assessments.	Achieve a cybersecurity awareness index of 75	

3.9 Objective 9

Ensure a consistent and high level of security across all MS by applying comprehensive cybersecurity policies and regulations while actively disseminate and communicate these standards and practices to ensure widespread adoption, foster collaboration with key stakeholders for effective policy contribution, exploitation, and standardization efforts and leverage the latest technologies and platforms to facilitate information exchange, knowledge sharing, and cybersecurity training across all sectors, enhancing the overall resilience and governance in cybersecurity throughout the MS.

Related module: CYBERGOPLUS

Verification: D6.3, D6.4, D9.3

Table 11: Objective 9 KPIs

KPI ID	Name	Description	Target	Measurement Methodology
KPI9.1	Policy Compliance Rate	Measure the level of compliance with EU-wide cybersecurity policies, regulations, and standards among MS.	Increase policy compliance rate to 65%.	Survey and assess the adoption rate of cybersecurity standards in various industries.

© CYberSynchrony, 2024

KPI9.2	Industry-specific Standard Adoption	Track the adoption rate of industry-specific cybersecurity standards and best practices by critical sectors	Increase rate to 65%	Survey and assess the adoption rate of cybersecurity standards in various industries.
KPI9.3	Cybersecurity Certification Rate	Measure the number of entities that have obtained cybersecurity certifications in alignment with EU-wide standards	Increase to 20 entities	
KPI9.4	Engagement in Dissemination and Communication (D&C) Activities	Engagement in Dissemination and Communication (D&C) Activities	Increase events by 30% annually	
KPI9.5	Stakeholder Engagement in Policy Contribution	Stakeholder Engagement in Policy Contribution	Onboard >= 50 new key stakeholders for policy input within three years.	
KPI9.6	Exploitation of CYberSynchrony Best Practices	Exploitation of CYberSynchrony Best Practices	Reach 60% adoption of CYberSynchrony best practices within three years.	

© CYberSynchrony, 2024

4 Use Case KPIs

4.1 Overview of Use Cases

UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare

Technology has become deeply embedded in healthcare, with digital imaging (X-rays, CTs, MRIs, ultrasounds) streamlining diagnostics, storage, and data sharing. However, as more sensitive data is digitized, hospitals, clinics, and research institutions are increasingly targeted by cyberattacks. Legacy IT systems lacking modern security, coupled with the rise of telemedicine, cloud platforms, and AI diagnostics, have significantly widened the attack surface. [1]

Critical Areas Needing Protection

- **Electronic Health Records (EHR/EMR):** Breaches can compromise patient safety by causing data loss or manipulation.
- **Telemedicine & Scheduling Systems:** Disruptions delay care and impact service delivery.
- **Internal Communications (Email, VoIP, Intranet):** Unauthorized access can lead to leaks or misinformation.
- **Billing & Financial Systems:** Targets for fraud and ransomware due to sensitive payment data.
- **Public Trust:** Cyber incidents damage reputations and erode patient confidence.
- **Guest & Staff Wi-Fi:** Poor segmentation can expose internal systems to attackers.

Key Challenges

- **Ransomware & Data Breaches:** Healthcare data is highly valuable to attackers.
- **Insecure Medical Devices (IoMT):** Many lack basic security.
- **Regulatory Compliance:** Strict obligations under GDPR, NIS2, and DORA.
- **Insider Threats & Human Error:** Limited staff awareness of cybersecurity risks.
- **Fragmented Security Tools:** Need for integrated threat detection and response.

Impact & Alignment with CYberSynchrony (UC1)

By addressing these challenges, we can reduce response times, limit damage from attacks, and ensure secure handling of patient data.

UC1 supports CYberSynchrony's goals by deploying and testing key components in a real healthcare setting:

- **CYRESCUE** for penetration testing
- **CYBERRA & CYBRITE** for risk monitoring and incident response
- **CROSS-CORE** for secure data exchange
- **CYBERWISE** for staff training
- **CYBERGOPLUS** for audits and compliance

Together, these tools enhance resilience and provide a replicable model for cybersecurity in healthcare.

UC2: CYberSynchrony-Powered Public Administration

Public institutions are rapidly digitizing services, from tax systems and ID management to digital voting and e-government portals. While this enhances efficiency and accessibility, it also exposes critical infrastructure to

© CYberSynchrony, 2024

cyber threats. Outdated systems, limited cybersecurity budgets, and complex bureaucratic environments increase vulnerability, making public administration a frequent target for nation-state actors, hacktivists, and ransomware groups.

Critical Areas Needing Protection

- **Citizen Data Registries:** Breaches can expose sensitive personal and national identity information.
- **E-Government Portals:** Disruptions affect access to essential services like licenses, benefits, and applications.
- **Internal Communication & Workflow Systems:** Attacks can paralyze day-to-day operations and delay decision-making.
- **Financial Systems:** Fraud or ransomware can compromise public funds and payment infrastructures.
- **Public Trust:** Cyber incidents can erode confidence in government institutions.
- **Third-Party Service Providers:** Unsecured vendors can become attack vectors.

Key Challenges

- **Legacy Systems & Technical Debt:** Many public IT systems lack current security updates.
- **Rising Threats from Sophisticated Actors:** Public sector is a prime target for politically motivated attacks.
- **Compliance Pressure:** Must meet evolving regulations like GDPR, NIS2, and national cybersecurity directives.
- **Lack of Cybersecurity Talent:** Skills shortages hinder response capability.
- **Coordination Across Agencies:** Fragmented governance can delay threat response and data sharing.

Impact & Alignment with CYberSynchrony (UC2)

UC2 enhances the cyber resilience of public administration by securing infrastructure, accelerating response, and protecting citizen data. It operationalizes CYberSynchrony components in a real-world government context:

- **CYRESCUE** for vulnerability testing
- **CYBERRA & CYBRITE** for monitoring and incident management
- **CROSS-CORE** for secure inter-agency data exchange
- **CYBERWISE** for staff training and simulations
- **CYBERGOPLUS** for auditing, compliance, and resilience assessments

This deployment strengthens digital trust in public services and offers a scalable cybersecurity model for public institutions across Europe.

UC3 Fortifying Universities with CYberSynchrony

Universities are dynamic, open environments with diverse users and complex IT needs. Their reliance on digital platforms for teaching, research, and administration makes them attractive targets for cyberattacks. Phishing, ransomware, and data breaches can disrupt operations, compromise research, and leak sensitive student or staff data. Academic networks are also highly interconnected, amplifying risk across institutional and cross-sector collaborations.

Critical Areas Needing Protection

© CYberSynchrony, 2024

- **Learning Management Systems (LMS):** Disruptions affect teaching continuity and access to course materials.
- **Student & Faculty Databases:** Contain personal, academic, and financial records vulnerable to breaches.
- **Research Data & IP:** Loss or theft can derail projects and compromise competitive advantage.
- **IT Infrastructure:** Targeted for lateral movement, data exfiltration, or service disruption.
- **Collaborative Networks:** Shared access with partners increases exposure to third-party risks.
- **Public Reputation:** Breaches can damage trust, affecting student recruitment and partnerships.

Key Challenges

- **Open Access Culture:** Balancing accessibility with robust security is difficult.
- **Legacy Systems:** Outdated tools remain common in academic IT environments.
- **Low Cyber Awareness:** Faculty, staff, and students often lack cybersecurity training.
- **Distributed Governance:** Decentralized decision-making hampers coordinated responses.
- **Budget Constraints:** Limited resources for cybersecurity investments.

Impact & Alignment with CYberSynchrony (UC3)

UC3 strengthens university cyber resilience by deploying and testing CYberSynchrony's security modules in real academic environments:

- **CYRESCUE** to identify network vulnerabilities
- **CYBERRA & CYBRITE** for monitoring and rapid incident response
- **CROSS-CORE** to secure data exchanges in research and administration
- **CYBERWISE** for training faculty, staff, and students
- **CYBERGOPLUS** for compliance, audits, and cyber maturity assessments

Led by UPRC, this use case will validate the adaptability of CYberSynchrony to higher education, offering a roadmap for safeguarding academic institutions and informing future cybersecurity efforts across public and private sectors.

4.2 KPIs per Use Case

Table 12: Use Case KPIs

KPI #	KPI	Target	CYberSynchrony Modules
UC1.KPI1	Data encryption	100% of successful data encryption implementation compared to the number of systems where encryption was previously not implemented	CROSS-CORE, CYBERGOPLUS
UC1.KPI2	Training in cybersecurity best practices	30 healthcare staff trained in cybersecurity best practises compared to the current staff with no training.	CYBERWISE

© CYberSynchrony, 2024

UC1.KPI3	Audit frequency & Critical findings	Increase audit frequency to bi-annually with a 50% reduction in critical findings after the first year of CYberSynchrony module implementation compared to previous frequency of audits (e.g., once a year) and past audit findings.	CYBERRA, CYBERGOPLUS
UC1.KPI4	Detection and Response time	Achieve a 60% reduction in detection and response time compared to the average time taken in past incidents.	CYBRITE, CYRESCUE, CYBERRA
UC2.KPI1	Number of incidents	Decrease the number of cybersecurity incidents detected and resolved by 20% compared to the past situation.	CYRESCUE, CYBRITE
UC2.KPI2	Response time	Decrease the time taken to respond to a cybersecurity incident by 20% compared to the current average time.	CYBRITE
UC2.KPI3	Staff compliance rates	Staff compliance rates with new cybersecurity protocols increased to 95% compared to the current rate of compliance.	CYBERWISE
UC2.KPI4	Digital IDs usage by citizens	Number of citizens using digital IDs for public services increased by 30% compared to the current situation.	CYBERRA, CROSS-CORE
UC3.KPI1	Number of incidents	Number of cybersecurity incidents detected and resolved decreased by 20% post-implementation.	Wazuh, Weka
UC3.KPI2	Faculty compliance rates	Faculty compliance rates with new cybersecurity protocols achieve 90% compliance post-training and awareness campaigns.	Wazuh, Weka
UC3.KPI3	Student cybersecurity satisfaction	Student satisfaction rates with new security of online services achieve 90% satisfaction post-enhancements.	Surveys, Feedback Analysis

© CYberSynchrony, 2024

UC3.KPI4	Response time	Time take to respond to cybersecurity incident reduced by 30% post SOAR platform deployment.	Wazuh, Snyk, Weka

© CYberSynchrony, 2024

5 Key Exploitable Results (KERs)

The partner consortium has opted for a tiered strategy to manage the knowledge generated. In this setup, the original knowledge creator retains the rights to their findings but shares the software execution with the entire consortium. The project's KERs will be made accessible as open-source community versions (with certain restrictions to prevent misuse) for academic and research communities to foster and expedite subsequent studies. Meanwhile, other outcomes provide notable commercial opportunities for consortium members. The preliminary plans for leveraging CYberSynchrony's KERs can be seen in Table 13 below, which will undergo further refinement throughout the project's tenure under the activities of T9.3. Exploitation and commercialization strategy. Next review of the KERs will be in D9.4, due in M18. For any KERs that multiple consortium members intend to monetize, prior agreements on IP/IPR will be made, and a unified commercialization approach, possibly in the form of a joint venture, will be rolled out in the designated market launch timeframe.

Table 13: Key Exploitable Results (KERs)

KERs	Whom	Type[2]	Licensing[3]	Service Type[4]	Time to market
CYberSynchrony Platform	All	S	CO	S, C, E	1-2 year(s) after project
CYRESCUE - Advanced Penetration Testing Tools	MAG, EBOS, IANUS, FP, BYTE, MER	S	CO	S, T, C, E	1-2 year(s) after project
CYRESCUE - SOAR Platforms	MAG, EBOS, IANUS, FP, BYTE, MER	PR	SaaS	S, T, C, E	1-2 year(s) after project
CYBERRA - Immutable Forensic Analysis Techniques	MAG, EBOS, IANUS, FP, BYTE, MER	PR	OA	S, T, C, E	1-2 year(s) after project
CYBERRA - Customized Risk Assessment Software	MAG, EBOS, IANUS, FP, BYTE, MER	P	C	S, T, C, E	1-2 year(s) after project
CYBRITE - Advanced Cybersecurity Analytics Tools	MAG, IANUS, TRUST, UPRC, FP, BYTE	P	C	S, T, C, E	1-2 year(s) after project
CYBRITE - SIEM Systems and Network Traffic Analysis Tools	MAG, IANUS, TRUST, UPRC, FP, BYTE	P	CO	S, T, C, E	1-2 year(s) after project
CROSS-CORE - Standardized Data Sharing Formats	MAG, IANUS, TRUST, BYTE, MER	S	S	S, T, C, E	1-2 year(s) after project
CYBERWISE - Cybersecurity Awareness Platforms with Gamification	ALL	S	SaaS	T, C	1-2 year(s) after project
CYBERWISE - Cybersecurity Awareness Training Initiatives	ALL	T	OA	T, C	1-2 year(s) after project

© CYberSynchrony, 2024

CYBERGOPLUS - Compliance Monitoring and Auditing Tools	ALL	P	C	S, T, C, E	1-2 year(s) after project
Cross-border Cyber Exercise Programs	ALL	S	SaaS	S, T, C, E	1-2 year(s) after project
Customized Cybersecurity Solutions	IANUS, TRUST, DSA, KETYAK, FP, BYTE, EGL, MER	S	SaaS	S, T, C, E	1-2 year(s) after project

© CYberSynchrony, 2024

6 KPI Dashboard Summary

Tabular representation of all KPIs:

Table 14: KPI Dashboard Summary

KPI ID	Name	Linked Objective, WP/UC	Target
KPI1.1	Number of Threat Assessments Carried Out	Obj 1	>36 threat assessments
KPI1.2	Number of Risk Scenario Analyses Carried Out	Obj1	>= 13 risk assessments
KPI1.3	Threat Intelligence platform effectiveness	Obj1	Detect & mitigate >85% of threats—85+ out of 100—within the set timeframe.
KPI1.4	Threat Intelligence platform Usability	Obj1	Raise user satisfaction to ≥4.5/5 MOS by improving usability & UX.
KPI1.5	Threat Intelligence platform Security	Obj1	Cut vulnerability remediation time to ≤15 days for faster, stronger security.
KPI1.6	Threat Intelligence platform Security Incident Response Time	Obj1	Cut response time to 4h for zero-days & 8h for others to ensure faster threat containment.
KPI2.1	Number of Penetration Tests Provided	Obj2	>= 60 penetration tests.
KPI2.2	Incident Detection Time	Obj2	Reduce the average incident detection time to 3 days.
KPI2.3	Incident Response Time	Obj2	Reduce the average incident response time to 15 days.
KPI2.4	Incident Resolution Rate	Obj2	Achieve at least a 80% incident resolution rate within 24 hours compared to last years
KPI3.1	Number of Threat Assessments Carried Out	Obj3	Conduct at least 36 threat assessments aiming to enhance the platforms' capabilities to identify and respond to emerging cyber threats promptly
KPI3.2	Number of Risk Scenario Analyses Carried Out	Obj3	Perform at least 13 risk scenario analyses aiming to improve risk assessment capabilities and enable more effective risk management and incident response strategies.
KPI3.3	Number of Potential Users Covered per Test/Exercise	Obj3	Increase the coverage to an average of 150 potential users per test/exercise
KPI3.4	Number and Nature of Vulnerabilities Discovered	Obj3	Reduce the number of high-severity vulnerabilities by 15% compared to other approaches while maintaining the overall discovery rate aiming to identify and address high-severity vulnerabilities more effectively

© CYberSynchrony, 2024

			without compromising the overall discovery efforts
KPI3.5	Threat Intelligence platform Security	Obj3	Reduce the platform vulnerability remediation time to 15 days aiming for faster remediation of vulnerabilities enhancing the platform's security posture.
KPI3.6	Risk Scenarios Analysed	Obj3	Increase the number of analysed risk scenarios by 15% aiming to analyse at least 12 customized risk scenarios to improve risk assessment capabilities.
KPI3.7	Risk Mitigation Index	Obj3	Achieve a 20% reduction in identified risks through more effective risk mitigation strategies aiming to improve the risk mitigation index and achieve better risk management outcomes.
KPI4.1	Number of Penetration Tests Provided.	Obj4	60 penetration tests plant (a 20% increase in tests to further validate security robustness aiming to reduce successful penetrations to 0, achieving a 0% success rate for the attackers while increasing the frequency of tests by 20%, while ensuring that each of the increased penetration attempts is successfully deterred.
KPI4.2	Number of Cross-Border Actions/Exercises	Obj4	10 cross-border actions/exercises aiming
KPI4.3	Vulnerabilities Addressed	Obj4	Address and remediate at least 80 vulnerabilities.
KPI4.4	Number and nature of Vulnerabilities Discovered	Obj4	Reduce the number of high-severity vulnerabilities by 15% compared to other approaches
KPI4.5	Incident Collaboration Index	Obj4	Increase the Incident Collaboration Index to 70%
KPI5.1	Number of Risk Monitoring Services Provided	Obj5	Activate 25 risk monitoring services while at least 95% of them should achieve a user satisfaction rating of 4 out of 5, based on criteria such as accuracy of threat detection, timeliness of alerts, and comprehensiveness of monitoring coverage and the false positive rate or these services should be < 5%, ensuring that the vast majority of alerts generated are relevant and actionable.
KPI5.2	Information Sharing Frequency	Obj5	Increase the information sharing frequency to 75% of cyber incidents and crises
KPI6.1	Number of Penetration Tests Provided	Obj5	60 penetration tests planned — a 20% increase to strengthen security and achieve

© CYberSynchrony, 2024

			a 0% attacker success rate, ensuring all attempts are effectively blocked.
KPI6.2	Number of Threat Assessments Carried Out	Obj6	> = 36 threat assessments
KPI6.3	Number of Risk Scenario Analyses Carried Out:	Obj6	>= 13 risk scenario analyses
KPI6.4	Vulnerabilities Addressed	Obj6	>= 80 vulnerabilities
KPI6.5	Threat Intelligence platform Security	Obj6	Reduce remediation Time to 15 days
KPI7.1	Number and Nature of Vulnerabilities Discovered	Obj7	Reduce by 15% compared to other approaches
KPI7.2	Vulnerabilities Addressed	Obj7	>= 80 vulnerabilities
KPI8.1	Cybersecurity Training Coverage	Obj8	Increase cybersecurity training coverage to 85%
KPI8.2	Cybersecurity Awareness Index	Obj8	Achieve a cybersecurity awareness index of 75.
KPI9.1	Policy Compliance Rate	Obj9	Increase policy compliance rate to 65%
KPI9.2	Industry-specific Standard Adoption	Obj9	Increase rate to 65%
KPI9.3	Cybersecurity Certification Rate	Obj9	Increase to 20 entities
KPI9.4	Engagement in Dissemination and Communication (D&C) Activities	Obj9	Increase events by 30% annually
KPI9.5	Stakeholder Engagement in Policy Contribution	Obj9	Onboard >= 50 new key stakeholders for policy input within three years.
KPI9.6	Exploitation of CYberSynchrony Best Practices	Obj9	Reach 60% adoption of CYberSynchrony best practices within three years.
UC1.KPI1	Data encryption	UC1	100% of successful data encryption implementation compared to the number of systems where encryption was previously not implemented
UC1.KPI2	Training in cybersecurity best practices	UC1	30 healthcare staff trained in cybersecurity best practises compared to the current staff with no training.
UC1.KPI3	Audit frequency & Critical findings	UC1	Increase audit frequency to bi-annually with a 50% reduction in critical findings after the first year of CYberSynchrony module implementation compared to previous frequency of audits (e.g., once a year) and past audit findings.
UC1.KPI4	Detection and Response time	UC1	Achieve a 60% reduction in detection and response time compared to the average time taken in past incidents.

© CYberSynchrony, 2024

UC2.KPI1	Number of incidents	UC2	Decrease the number of cybersecurity incidents detected and resolved by 20% compared to the past situation.
UC2.KPI2	Response time	UC2	Decrease the time taken to respond to a cybersecurity incident by 20% compared to the current average time.
UC2.KPI3	Staff compliance rates	UC2	Staff compliance rates with new cybersecurity protocols increased to 95% compared to the current rate of compliance.
UC2.KPI4	Digital IDs usage by citizens	UC2	Number of citizens using digital IDs for public services increased by 30% compared to the current situation.
UC3.KPI1	Number of incidents	UC3	Number of cybersecurity incidents detected and resolved decreased by 20% post-implementation.
UC3.KPI2	Faculty compliance rates	UC3	Faculty compliance rates with new cybersecurity protocols achieve 90% compliance post-training and awareness campaigns.
UC3.KPI3	Student cybersecurity satisfaction	UC3	Student satisfaction rates with new security of online services achieve 90% satisfaction post-enhancements.
UC3.KPI4	Response time	UC3	Time needed to respond to cybersecurity incident reduced by 30% post SOAR platform deployment.

Table 15 and Table 16 below outline the Dissemination and Communication KPIs, target values, and status of achievement as of April 2025, respectively.

Table 15: Communication KPIs, targets and status

#	Communication KPI	Target	Status
C.1	**Project Website** (M03- 6 years)		
C.1.1	Project website running from M03- 6 years	Published by M03	1.7K unique users
C.2	**Social Media** (M01-M36)		
C.2.1	Followers by M36	> 1000	176
C.2.2	Average monthly impressions	>500	618
C.3	**e-Newsletters and Email Campaigns** (From M06)	Bi-annually	
C.3.1	Newsletters	>10	1
C.3.2	Total contacts on mailing list	>1000	52
C.4	**Online Publishing** (M06-M36)		
C.4.1	Press Releases	≥12	4
C.4.2	Published articles in newspapers, magazines, and online	≥10	
C.5	**Blogs, fora** (M12-M36)		

© CYberSynchrony, 2024

C5.1	Unique blog publications/contributions	>10	
C5.2	Different platforms for posting	>4	
C.6	**Promotional Material** (From M06-M36)		
C.6.1	Printed materials (e.g., brochures, flyers)	>3000	1 roll-up banner
C.6.2	Display banners	>3	
C.7	**Multimedia** (M09-M36)		
C.7.1	Produced Videoclips	3	
C.7.2	Views	> 10000	
C.7.3	Conducted interviews	>6	
C.8	**Public Talks** (M09-M36)		
C.8.1	Public events at Universities	>3 (Participants >60)	4
C.8.2	University Open Days	>3	1
C.8.3	Events hosted by local entities and societal stakeholders	>4 (>120 participants)	2

Table 16: Dissemination KPIs, targets, and status

#	Dissemination KPI	Target	Status
D.1	**Co-organisation and/or participation to events**		
D.1.1	Use case-based workshops	3	
D.1.2	Training Program	1	
D1.3	Showcases	>2	1
D1.4	Webinars	>6 (>40 Participants each)	1
D.1.5	Exhibitions/trade fairs/symposiums	>3	
D.2	**Scientific presentations**		
D.2.1	Scientific papers	>6	3
D.2.2	Presentations in Scientific Conferences	>6	2
D.3	**Bodies to disseminate project results**		
D.3.1	High-impact communities/associations where to push results	>2	
D.4	**Standardization Bodies and Open-Source Initiatives**		
D.4.1	Number of standardisation contributions to different SDOs with adoption status	>1	

© CYberSynchrony, 2024

7 Deviations and Mitigation Measures

As of the current reporting period, the CYberSynchrony project remains in its foundational phase, focused on preparatory actions, infrastructure setup, and methodological alignment. Given this early stage, no significant deviations from the Grant Agreement have been formally identified. However, several **potential risks** and **observations** have emerged that warrant proactive attention to ensure smooth KPI implementation in future phases.

7.1 Potential or Anticipated Deviations

- **Delayed Availability of Pilot Data:** Due to the complex integration processes within healthcare, public administration, and academic institutions, additional time is required to establish data collection protocols for some use case environments. This could delay the initial benchmarking of specific KPIs related to incident response, platform usability, and training effectiveness.
- **Alignment of KPI Methodologies Across WPs:** While the KPI definitions have been successfully established, variations in technical readiness across different work packages may affect the uniformity of initial KPI validation.
- **Cross-border Coordination Complexity:** As outlined in WP8 and WP9, the implementation of joint exercises and mutual assistance protocols involves administrative and legal harmonization across multiple Member States, which may introduce delays in reaching targets tied to cross-border cooperation KPIs.

7.2 Mitigation Measures

In response to these early signals, the project has introduced the following mitigation strategies:

- **Flexible Timeline Adjustments:** For KPIs dependent on pilot deployments, internal buffers have been accounted for in upcoming deliverables to allow for staged deployment without compromising quality.
- **Continuous Monitoring via KPI Dashboard:** The central dashboard outlined in Chapter 6 of this report enables real-time oversight of KPI readiness and supports early identification of underperformance risks.
- **Stakeholder Coordination Workshops:** Cross-WP alignment is being strengthened through regular joint coordination meetings, where KPI-related inputs and dependencies are reviewed and refined.
- **Standardized Data Collection Protocols:** Common templates and methodologies, are being disseminated to all partners to streamline future reporting and ensure consistency.

Where applicable, any **significant deviations** that impact the contractual obligations defined in the **Grant Agreement (GA 101158555)** will be addressed formally and reported in the upcoming periodic technical reports. Minor adjustments to internal milestones or interpretation of certain KPIs are being managed within the project's governance framework without requiring formal amendments at this stage.

© CYberSynchrony, 2024

8 Conclusions

This deliverable marks a critical milestone in the CYberSynchrony project, establishing a comprehensive framework for monitoring KPIs aligned with the project's strategic objectives and operational use cases. While the project is still in its first year, significant progress has been made in defining the full KPI set, linking them to the Grant Agreement commitments and implementing the initial mechanisms required for consistent tracking and evaluation.

Key achievements of this report include:

- A detailed mapping of KPIs to the project's 9 objectives and 3 use cases.
- Development of standard methodologies for KPI measurement and reporting.
- Integration of KPI tracking into the project's quality assurance and risk management systems.
- Initial alignment of technical deliverables and use case plans to support KPI data collection in future phases.

Though no quantitative KPI outcomes are expected at this stage, the deliverable provides a solid basis for future measurement, enabling the consortium to proactively monitor progress and address potential risks as they arise.

Going forward, the KPI dashboard and the methodologies documented in this report will be instrumental in driving project-wide alignment, ensuring transparency, and supporting evidence-based decision-making. As the CYberSynchrony platform transitions from design to deployment, these KPIs will serve as essential benchmarks for evaluating the project's impact, scalability and long-term sustainability across the European cybersecurity ecosystem.

© CYberSynchrony, 2024

9 References

[1] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.

© CYberSynchrony, 2024