



CYberSynchrony

Harmonizing People, Processes, and Technology for Robust Cybersecurity

Dr Violeta Vasileva (MAG),
Demetris Antoniou (IANUS)

ENISA ECSF Workshop
Brussels, 20th November



This project has received funding by the European Union's Digital Europe programme 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 European Cybersecurity Competence Centre can be held responsible for them.

SUMMARY

This presentation shows research on Europe's evolving cybersecurity landscape and sector-specific challenges in healthcare, administration, and academia. It showcases how these insights guide the design of modular, adaptable components that strengthen resilience, compliance and skills across critical sectors.

Agenda

Outline

01

A brief overview of
CyberSynchrony

02

Pilot Areas – Sector-specific
Findings and Skills Needs

03

Technical Overview

04

Integration of ECSF

About the Project



Building a flexible and comprehensive cybersecurity framework that brings together cutting-edge technologies to create a stronger, more connected defense system. By combining technical innovation, human expertise and efficient processes, the project helps organizations build a security-first culture and respond quickly to cyber incidents. A key part of CYberSynchrony is its support for small and medium-sized enterprises (SMEs) through Financial Support to Third Parties (FSTP), helping them strengthen their cybersecurity capabilities and become part of a more resilient digital ecosystem.

Project's Statistics



Action Grant
Total Budget
6 998 153.10



Consortium



MAGGIOLI SPA (MAG)



EBOS TECHNOLOGIES LIMITED
(eBOS)



IANUS TECHNOLOGIES LTD
(IANUS)



TRUSTILIO BV (TRUST)



UNIVERSITY OF PIRAEUS
RESEARCH CENTER (UPRC)



DIGITAL SECURITY AUTHORITY
(DSA)



ETHNIKI YPIRESIA PLIROFORION
(KETYAK)



FOCAL POINT (FP)



BYTE COMPUTER ANONYMI
VIOMICHANIKIEMPORIKI
ETAIREIA (BYTE)



DIMOS EGALEO (EGL)



MERIDIAN SRL (MER)



APOSTOLOS LOUKAS MEDICAL
CENTRE (AMC)

Methodology

Phase 1

Analysing Cybersecurity Terrain & MS Requirements

This phase focuses on understanding user needs, defining specific scenarios, and designing the toolkit's structure. It also considers legal, societal, and human factors affecting cybersecurity threat detection.

Phase 3

Confluence, Showcasing, Capacity Building and Open Calls

This phase enhances the CYberSynchrony platform, focusing on training, adoption, and connecting experts with SMEs. The Open Call invites contributions of innovative cybersecurity tools, offering financial support, mentorship, and visibility to selected participants, ensuring the platform remains cutting-edge and impactful.

Phase 2

Shaping the CYberSynchrony Ecosystem & Infrastructure

This stage focuses on designing and refining system components, integrating tools, and aligning the CYberSynchrony platform with the ENISA Threat Landscape and global standards. Insights from use-case collaborations with MS and user feedback shape the ecosystem, ensuring user-centric recommendations that support the project's educational goals.

Use Cases



Use Case 1

**Demonstrating
Comprehensive CyberHealth
Security for Digital
Healthcare**



Use Case 2

**CYberSynchrony-Powered
Public Administration**



Use Case 3

**Fortifying Universities with
CYberSynchrony**



Digital Healthcare



Use Case 1

Demonstrating Comprehensive CyberHealth Security for Digital Healthcare

The integration of **technology into healthcare** has ushered in breakthroughs in medical devices and AI, optimizing treatments and monitoring. However, this digital shift brings concerns about the susceptibility of interconnected devices to cyberattacks, **jeopardizing patient safety and healthcare system integrity**. These challenges arise from design flaws and inadequate security measures in devices. Modern healthcare is strained by potential cyberattacks, impacting patient care and exposing the inadequacies of current security solutions. Since the COVID-19 outbreak, there's been a notable surge in cyberattacks on health facilities.



www.cybersynchrony.eu

 cybersynchrony

 @c_yber1007

 @CYberSynchrony

Objectives



Use Case 1

Demonstrating
Comprehensive CyberHealth
Security for Digital
Healthcare

1

Implementation robust encryption methods to secure sensitive patient data.

2

Conduct regular cybersecurity audits and risk assessment of healthcare IT systems.

3

Establish a real-time monitoring system for detecting unauthorized activities and potential data breaches.

4

Develop and implement a comprehensive incident response plan for cybersecurity threats.

5

Train healthcare staff in cybersecurity best practises and awareness.



Public Administration



Use Case 2

CYberSynchrony-Powered Public Administration

Public administrations play a **crucial role** in delivering services to citizens, making their cybersecurity paramount for maintaining public trust, national security, and efficient governance. In an era of increasing cyberattacks, with a **600% surge** and **95% of breaches** attributed to human errors, the introduction of secure e-governance platforms is essential. However, public administrations face challenges like **outdated legacy systems**, which lack modern defences, and the responsibility of safeguarding sensitive personal and national security data. Financial constraints, the absence of specialized expertise, and ensuring **coordinated cybersecurity efforts** across departments further compound these challenges.



Objectives



Use Case 2

CYberSynchrony-Powered Public Administration

1

Safeguard the integrity and security of online services offered to the public.

2

Implement digital IDs for secure and efficient citizen identification.

3

Use blockchain technology for tamper-proof public records.

4

Develop and implement a comprehensive incident response plan for cybersecurity threats.

5

Train public administration staff in cybersecurity best practices and awareness.



University



Use Case 3

Fortifying Universities with CYberSynchrony

Universities prioritize protecting intellectual property and ensuring **students' digital safety**. They also strive for uninterrupted academic and administrative operations and compliance with **data protection mandates**. However, they face challenges in enhancing cybersecurity due to budget constraints, diverse demographics with varied tech skills, and multifaceted IT ecosystems. The **dependence on external platforms** for various services further complicates security, as ensuring third-party compliance with **university security standards** is challenging.



Objectives



Use Case 3

Fortifying Universities with CYberSynchrony

1

Guarantee the integrity and safety of e-learning platforms utilized by the institution.

2

Put in place strong digital security measures to safeguard critical research data.

3

Ensure the confidentiality and integrity of student academic and personal records.


4

Equip teaching staff with the knowledge and skills needed for cybersecurity best practices.

5

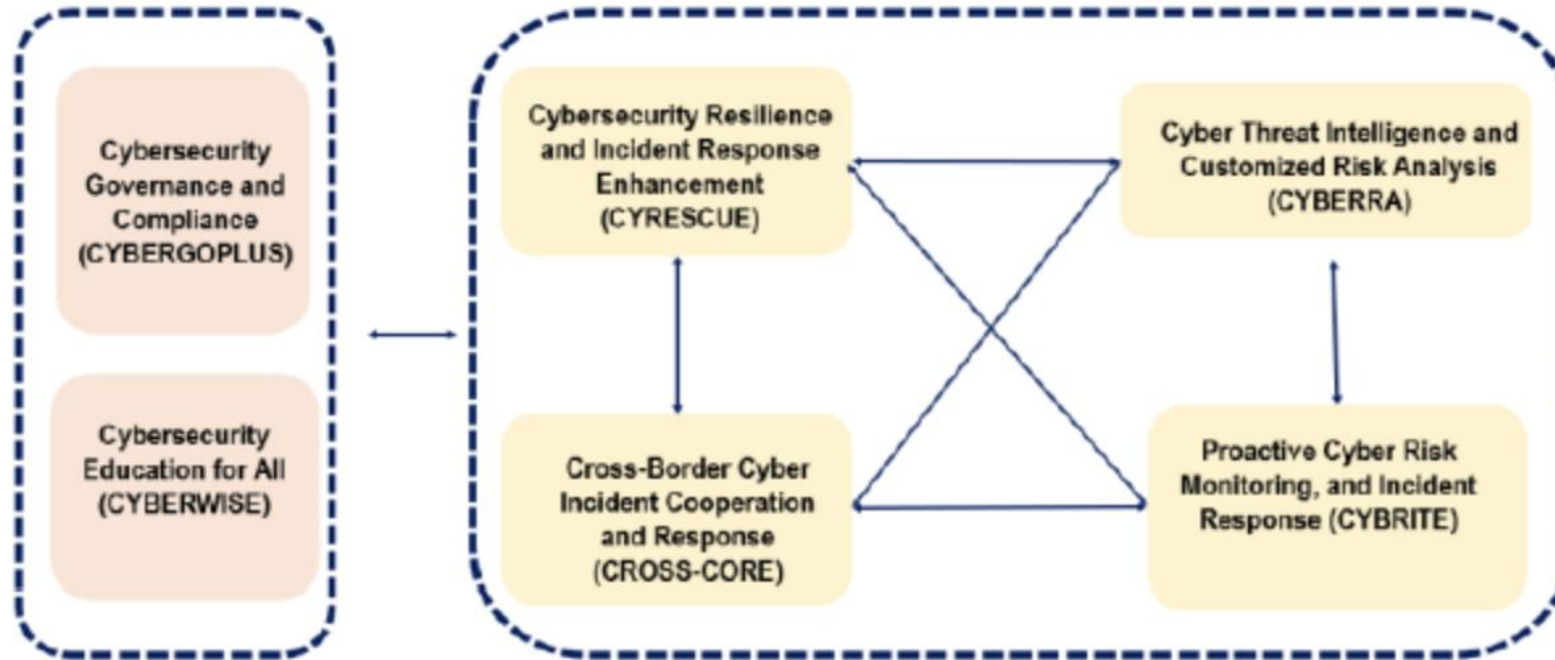
Formulate and execute a detailed plan for handling cybersecurity incidents.





CYberSynchrony Technical Overview

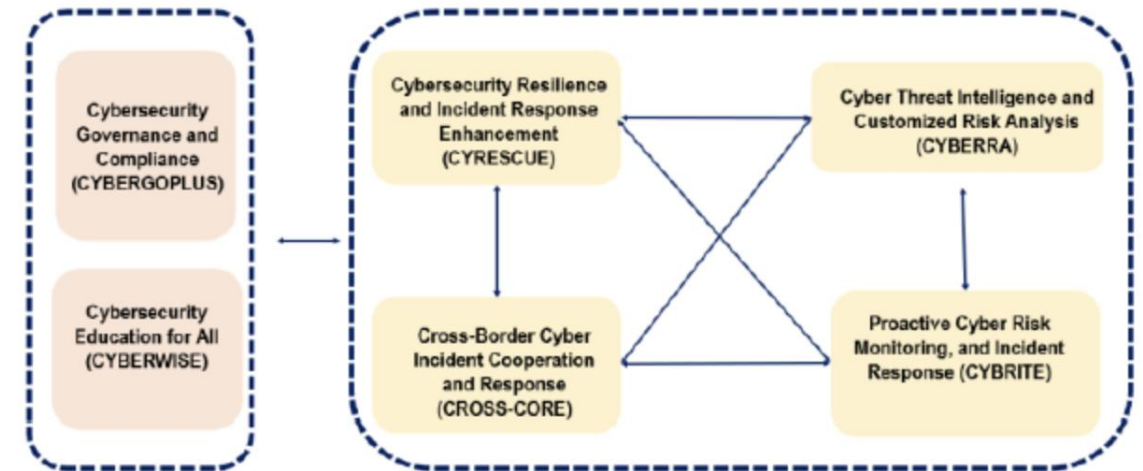
A brief overview of the CyberSynchrony Project



CYberSynchrony is a Modular Cybersecurity Framework (MCF) that includes people, processes, and culture proposing an ecosystem that integrates innovative technologies in order to achieve a more robust, resilient and interconnected cybersecurity infrastructure

CyberSynchrony Modules – High-Level Overview

1. **CYBERRA**: Real-time cyber threat intelligence and tailored risk analysis to support MS' situational awareness.
2. **CYRESCUE**: Vulnerability identification, penetration testing and automated incident response using threat simulation toolkits.
3. **CYBRITE**: Proactive threat detection and incident response through continuous monitoring, anomaly detection and analytics.
4. **CROSS-CORE**: Cross-border collaboration through blockchain-based evidence validation, standardized data exchange and federated sharing.
5. **CYBERWISE**: Promotes cybersecurity awareness via interactive educational platforms and gamified training
6. **CYBERGOPLUS**: Supports the development and enforcement of cybersecurity policies, standards, and regulatory compliance tools across sectors.



The ECSF in the Project

Cybersecurity
Governance and
Compliance
(CYBERGOPLUS)

Understanding the Governance, Risk, and Compliance aspects of a holistic information security solution requires an understanding of the relevant processes **and the necessary skills to perform them.**

Example - Tech Speech:

The internal communications use TLS 1.1 which is depreciated and is actively exploited in the wild.



Example - GRC Speech:

We use outdated technologies which can compromise our compliance with the GDPR, and we could be sanctioned



The ECSF Questionnaire

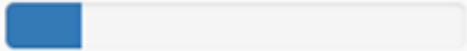
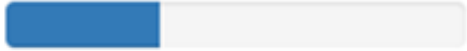
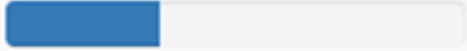

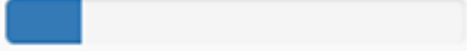
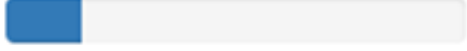
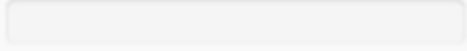
Which cybersecurity skill areas are currently missing or underrepresented in your organization?

Select all that apply, not all roles might be applicable to your organization

Chief Information Security Officer (CISO) Leads the cybersecurity strategy, aligns it with business goals, and ensures governance and oversight of the cybersecurity function.	50.00 %
Cyber Legal, Policy & Compliance Officer Ensures the organization complies with cybersecurity laws, regulations, and standards; translates legal requirements into operational policies.	33.33 %

Questionnaire Outcomes

9. Has your organization experienced difficulties in recruiting or retaining staff with cybersecurity expertise? Select all that apply:

		Ratio
We have not experienced any issues in hiring or retaining cybersecurity staff		16.67 %
We face challenges hiring staff with specialized technical skills (e.g., incident response, threat analysis)		33.33 %
We face challenges hiring staff with governance/risk/compliance skills		33.33 %
Retention of skilled cybersecurity staff is difficult due to market demand		50.00 %
We rely on external consultants or service providers for cybersecurity expertise		16.67 %
Other		16.67 %
No Answer		0.00 %

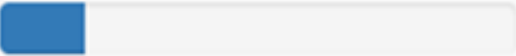

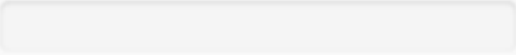
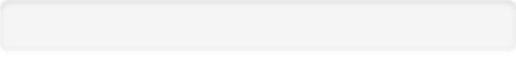
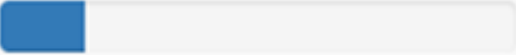
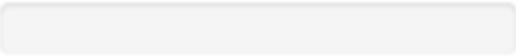
Questionnaire Outcomes

7b. Optional: In your opinion, what type of reporting would enable executive management to make more informed decisions regarding cybersecurity risk? (Open-ended response)



Questionnaire Outcomes

8. Are the cybersecurity reports presented to the Board or executive management standardized and repeatable (i.e., based on predefined formats or templates)?

		Ratio
Yes, reports follow a standardized format with predefined metrics		16.67 %
Partially — some elements are standardized, others are ad hoc		66.67 %
No, reports are created on an ad hoc basis depending on the audience or issue		0.00 %
No formal reporting has taken place		0.00 %
Other		16.67 %
No Answer		0.00 %

Derived Requirements

Governance & Compliance Requirements

- Insights show weak GRC maturity and inconsistent NIS2 alignment.
- System must include governance workflows, compliance guidance, and standardised reporting.

Skills & Training Requirements

- Workforce gaps mapped to ECSF profiles
- System must deliver embedded training hooks, role-based guidance, and continuous upskilling pathways.

Operational Requirements

- Need for clearer metrics and executive visibility.
- System must unify operational telemetry and provide cross-sector KPIs.

Q & A



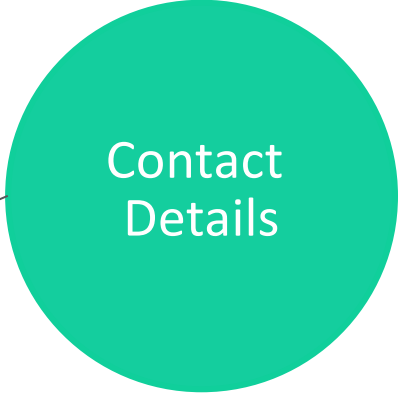
Dr Violeta Vasileva



Gruppo Maggioli (IT/GR)



violeta.vasileva@maggioli.gr



Contact
Details