# Harmonizing People, Processes, and Technology for Robust Cybersecurity

# D8.1 CYberSynchrony Integration Blueprint & Use Case Portfolio 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** | D8.1 CYberSynchrony Integration Blueprint & Use Case Portfolio V1 | | |
| **Work Package** | WP8 Integration, Demonstration, and evaluation | | |
| **Contractual due date** | 31 May 2025 | **Actual submission date** | 30 May 2025 |
| **Type** | R – Document, Report | **Dissemination Level** | PU - Public |
| **Lead Beneficiary** | eBOS | | |
| **Responsible Author** | Panayiotis Klitou (eBOS) | | |
| **Contributions from** | Revaz Berozashvili (eBOS), Charalambos Klitis (eBOS), Alexandros Psychas (MAG), Evangelos Michos (IANUS), Laskarina Mavropoulou (MER), Andrea Purificato (MER), Dimitris Koutras (FP), Leandros Maglaras (TRUST), George Karavokiros (BYTE), Athina Skarpeti (AMC), Dionissis Skarpetis (AMC), Platon Rizopoulos (EGL), Spiros Papagianopoulos (UPRC) | | |

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. 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 | 06.03.2025 | Initial Deliverable structure | Panayiotis Klitou (eBOS) |
| 0.2 | 20.03.2025 | Initial content | Panayiotis Klitou (eBOS) |
| 0.3 | 24.03.2024 | Contribution to 3.3 | Laskarina Mavropoulou (MER) |
| 0.4 | 11.04.2024 | Finalisation of eBOS' sections | Panayiotis Klitou (eBOS) |
| 0.5 | 25.04.2025 | Contribution as Technical Manager | Evangelos Michos (IANUS) |
| 0.6 | 28.04.2025 | Contributions from FP, BYTE, TRUST to Chapter 3 | Dimitris Koutras (FP), Leandros Maglaras (TRUST), George Karavokiros (BYTE) |
| 0.65 | 02.05.2025 | Contribution for Chapters 5, 6, 7 from UC leaders | Athina Skarpeti (AMC), Platon Rizopoulos (EGL), Spiros Papagianopoulos (UPRC) |
| 0.7 | 08.05.2025 | Contribution to section 3 (Deployment architecture, tool interactions) | Alexandros Psychas (MAG) |
| 0.8 | 09.05.2025 | Completion of draft for peer review | Panayiotis Klitou (eBOS) |
| 0.9 | 16.05.2025 | Peer review & QA review completed | Leandros Maglaras (TRUST), Spiros Papagianopoulos (UPRC), Charalambos Klitis (eBOS) |
| 0.95 | 27.05.2025 | Addressing peer review comments | Panayiotis Klitou (eBOS), Athina Skarpeti (AMC), Platon Rizopoulos (EGL), Spiros Papagianopoulos (UPRC) |
| 1.0 | 29.05.2025 | Final version ready for submission | Panayiotis Klitou (eBOS) |

***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 ..... 9
2 Introduction ..... 10
2.1 Mapping CYberSynchrony Outputs ..... 10
2.2 Linkage to other project outputs ..... 11
2.3 Deliverable Structure ..... 12
3 Methodology for Integrating the CYberSynchrony marketplace ..... 14
3.1 Integration roadmap ..... 15
3.2 Integration methodology ..... 17
3.2.1 High-level architecture description ..... 17
3.2.2 Definition of tools and relevance to the integration work ..... 19
3.3 Overview of Components (Tools) ..... 21
3.3.1 Communication Interfaces and Data Exchange ..... 22
3.4 Programming Languages and Technologies Used ..... 23
3.4.1 Architecture of Kubernetes ..... 25
3.4.2 Integration and Interoperability in Kubernetes ..... 25
3.4.3 Frontend–Backend Integration Methodologies ..... 26
4 Methodology for Testing the CYberSynchrony marketplace ..... 29
4.1 Testing Methodology ..... 29
5 UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare ..... 32
5.1 Use Case information ..... 32
5.2 System Architecture and Assets Identification ..... 33
5.3 Current Security Mechanisms ..... 38
5.4 CYberSecurity Awareness Program ..... 38
5.5 UC1 KPIs and Objectives ..... 39
5.6 Scenario Definition ..... 41
6 UC2: CYberSynchrony-Powered Public Administration ..... 45
6.1 Use Case information ..... 45
6.1.1 Needs and Motivation ..... 45
6.1.2 Relevance to CyberSynchrony ..... 45
6.2 System Architecture and Assets Identification ..... 47
6.3 Current Security Mechanisms ..... 49
6.4 CYberSecurity Awareness Program ..... 50
6.5 UC2 KPIs and Objectives ..... 51
6.6 Scenario Definition ..... 52
7 UC3: Fortifying Universities with CYberSynchrony ..... 58
7.1 Use Case information ..... 58
7.1.1 Use Case Needs & Motivation ..... 58
7.1.2 UC3 Description ..... 58
7.1.3 Relevance to CYberSynchrony ..... 58
7.1.4 Roles related to testing and evaluation within UC3 ..... 58
7.2 System Architecture and Assets Identification ..... 59
7.3 Current Security Mechanisms ..... 65
7.4 CYberSecurity Awareness Program ..... 65
7.5 UC3 KPIs and Objectives ..... 66
7.6 Scenario Definition ..... 67
8 Conclusions ..... 73
9 References ..... 74
Annex I: Tools communication matrix ..... 75

© CYberSynchorny, 2024

# List of Figures

Figure 1: Integration roadmap of the CYberSynchrony Platform ..... 16
Figure 2: CYberSynchrony Deployment architecture ..... 17
Figure 3: Technical Plan excel file ..... 20
Figure 4: (a) Kubernete's architecture, visualising the different components and interactions, (b) Sheduler assigning pods to available nods ..... 25
Figure 5: Healthcare Infrastructure – External ..... 33
Figure 6: Healthcare Infrastructure – Internal ..... 34
Figure 7: Storage Equipment – NAS ..... 35
Figure 8: Storage Equipment – PACS ..... 36
Figure 9: UC2 infrastructure architecture diagram ..... 47
Figure 10: High-Level Architectural Diagram ..... 61
Figure 11: High-Level Network Diagram ..... 62
Figure 12: University Network Infrastructure and Network ..... 64

# List of Tables

Table 1: Adherence to CYberSynchrony's GA ..... 10
Table 2: Links to other Project Outputs/Work ..... 12
Table 3: Explanation of the collected fields of the Technical Plan excel file ..... 19
Table 4: Tools overview: deployment location and component interfaces ..... 21
Table 5: Description of data exchanged between the tools ..... 22
Table 6: Comparison of virtual machines, docker containers, and Kubernetes ..... 24
Table 7: Comparison of integration methodologies ..... 27
Table 8: Roles and Responsibilities within UC1 ..... 33
Table 9: UC1 assets description ..... 37
Table 10: List of UC1 security mechanisms. ..... 38
Table 11: UC1 status of cybersecurity awareness ..... 38
Table 12: UC1 KPIs and target values ..... 39
Table 13: UC1 Objectives and mapping to KPIs ..... 39
Table 14: UC1 Test Scenario 1 ..... 42
Table 15: UC1 Test Scenario 2 ..... 42
Table 16: UC1 Test Scenario 3 ..... 43

© CYberSynchorny, 2024

Table 17: UC1 Test Scenario 4 ..... 43
Table 18: Roles and Responsibilities within UC2 ..... 46
Table 19: List of UC3 security mechanisms. ..... 50
Table 20: UC2 status of cybersecurity awareness ..... 50
Table 21: UC2 KPIs and target values ..... 51
Table 22: UC2 Objectives and mapping to KPIs ..... 51
Table 23: UC2 Test Scenario 1 ..... 52
Table 24: UC2 Test Scenario 2 ..... 53
Table 25: UC2 Test Scenario 3 ..... 54
Table 26: UC2 Test Scenario 4 ..... 56
Table 27: Roles and Responsibilities within UC3 ..... 59
Table 28: UC3 assets description ..... 59
Table 29: List of UC3 security mechanisms. ..... 65
Table 30: UC3 status of cybersecurity awareness ..... 66
Table 31: UC3 KPIs and target values ..... 66
Table 32: UC3 Objectives and mapping to KPIs ..... 67
Table 33: UC3 Test Scenario 1 ..... 68
Table 34: UC3 Test Scenario 2 ..... 69
Table 35: UC3 Test Scenario 3 ..... 70
Table 36: UC3 Test Scenario 4 ..... 71

© CYberSynchorny, 2024

# Acronyms and abbreviations

| Abbreviation / Term | Description |
|---|---|
| API | Application Programming Interface |
| CAS | Central Authentication Service |
| CI | Continuous Integration |
| CSV | Comma-Separated Values |
| DB | Database |
| DHCP | Dynamic Host Configuration Protocol |
| DLT | Distributed Ledger Technology |
| DDoS | Distributed Denial of Service |
| DNS | Domain Name System |
| EHR | Electronic Health Record |
| GA | Grant Agreement |
| GDPR | General Data Protection Regulation |
| HMI | Human-Machine Interface |
| HRM | Human Resource Management |
| IDS | Intrusion Detection System |
| IoMT | Internet of Medical Things |
| IP | Internet Protocol |
| JSON | JavaScript Object Notation |
| KPI | Key Performance Indicator |
| LMS | Learning Management System |
| MCF | Modular Cybersecurity Framework |
| MFA | Multi-Factor Authentication |
| MISP | Malware Information Sharing Platform |
| NIS2 | Network and Information Security Directive |
| NOC | Network Operations Center |
| PACS | Picture Archiving and Communication System |
| RBAC | Role-Based Access Control |
| REST | Representational State Transfer |
| SAN | Storage Area Network |

© CYberSynchorny, 2024

| | |
|---|---|
| SIEM | Security Information and Event Management |
| SIS | Student Information System |
| SLA | Service Level Agreement |
| SNYK | Security Analysis Tool for Vulnerabilities |
| SOAR | Security Orchestration, Automation, and Response |
| SQL | Structured Query Language |
| SSO | Single Sign-On |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UBA | User Behavior Analytics |
| UC | Use Case |
| VM | Virtual Machine |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAF | Web Application Firewall |
| WP | Work Package |
| XML | Extensible Markup Language |

© CYberSynchorny, 2024

# 1 Executive Summary

Deliverable D8.1 – CYberSynchrony Integration Blueprint & Use Case Portfolio v1, part of WP8 – Integration, Demonstration, and Evaluation, is a strategic response to the project's goal of fortifying cyber defence mechanisms. It provides a comprehensive, step-by-step roadmap for integrating the CYberSynchrony modules into the organisation's existing infrastructure. As the initial version delivered in M12, it lays the groundwork for the final blueprint scheduled for completion in M36.

The deliverable is structured around two interrelated components:

- **Integration Blueprint:**

This component details the technical and organisational roadmap required to merge the various CYberSynchrony modules into a unified, efficient, and robust cybersecurity ecosystem. It encompasses deployment processes, technical specifications, and the practical measures essential for seamless integration into the current infrastructure. By building on early work from D2.1, this updated architecture outlines the communication protocols, data exchange mechanisms, and defined interfaces between the different CYberSynchrony tools. Additionally, it discusses the programming tools and methodologies employed in constructing the platform.

- **Use Case Portfolio:**

In parallel, the deliverable offers a curated collection of tailored use cases (UCs) that illustrate how the integrated platform can be deployed in real-world scenarios. It specifically demonstrates the plan for evaluation of the platform within three critical application domains. Each use case is designed to align with the CYberSynchrony objectives, showcasing tangible improvements in cyber defence and establishing clear links between the platform's functionalities and the corresponding Key Performance Indicators (KPIs).

This first version of the deliverable, D8.1, reports on the preliminary efforts within WP8, with a dedicated focus on both the integration and the practical evaluation of the CYberSynchrony ecosystem. In relation to Task 8.1, the deliverable provides an integration roadmap aimed at leveraging the CYberSynchrony platform to its full potential. It describes the updated architecture for the platform—detailing communication, data exchange, and interface strategies—while also outlining the programming tools and methodologies that underpin its development. Furthermore, it presents the ongoing work in use case planning by compiling a portfolio that demonstrates the integration approach for three organisations and outlines a strategy for evaluating platform functionalities in line with the use cases' KPIs and objectives.

By concentrating on both integration and demonstration/evaluation, this deliverable not only captures the technical dimensions of embedding the CYberSynchrony platform but also validates its practical effectiveness through real-world application scenarios. The Integration Blueprint ensures a smooth adoption process, while the Use Case Portfolio substantiates the platform's operational value across diverse sectors.

© CYberSynchorny, 2024

# 2 Introduction

CYberSynchrony aims to establish a Modular Cybersecurity Framework (MCF) that integrates people, processes, and culture within an ecosystem enhanced by innovative technologies—delivering a robust, resilient, and interconnected cybersecurity infrastructure. This holistic framework addresses every facet of organisational security through a synergy of advanced technological solutions, active human involvement, systematic processes, and a security-centric culture. As a result, stakeholders can anticipate improved security, greater operational efficiency, enhanced collaboration, heightened cyber awareness, reliable regulatory compliance, and adaptable solutions that evolve in line with emerging cyber threats.

To realise these objectives, the project introduces the CYberSynchrony Platform—a comprehensive modular ecosystem composed of several interconnected modules and tools, each designed with specific technological capabilities and targets to bolster cybersecurity resilience and foster a culture of cyber awareness.

This deliverable outlines the roadmap for integrating these diverse tools into distinct modules and ultimately leveraging the complete CYberSynchrony platform. It details the stages toward achieving full integration, with a focus on establishing effective communication and data exchange protocols among the modules. The deliverable presents an updated architectural framework that specifies where each tool resides, delineates the data flow between components, and identifies the interfaces connecting the tools. This work builds on the early architecture and tool information developed in WP2, specifically in D2.1, and further elaborates on the integration strategy and the programming tools and methodologies needed for successful implementation.

The second segment of this deliverable is dedicated to the demonstration and evaluation of the CYberSynchrony platform. This part is centred on unlocking the platform's full operational potential to address a broad spectrum of end-user cybersecurity needs, with a particular emphasis on threat awareness and training. Validation, demonstration, and evaluation efforts are concentrated on three key sectors, reflected in the project's use cases:

- UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare
- UC2: CYberSynchrony-Powered Public Administration
- UC3: Fortifying Universities with CYberSynchrony

In this document, a detailed portfolio for these three use cases—developed from the initial definitions in D2.1—is presented. The portfolio illustrates how each use case aligns with CYberSynchrony's core objectives and offers a holistic, robust approach to enhancing cyber defence mechanisms. Additionally, a comprehensive plan for integrating the CYberSynchrony platform within the organisations linked to each use case is provided. This plan ensures system compatibility and identifies potential integration challenges or vulnerabilities during testing. A comprehensive validation methodology is also outlined, which links each use case's objectives to corresponding KPIs, identifies the specific platform modules that will undergo testing, and details targeted test scenarios. The use case portfolios are discussed in detail in Chapters 5, 6, and 7.

## 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** | | | |

© CYberSynchorny, 2024

| | | | |
|---|---|---|---|
| D8.1 | **CYberSynchrony Integration Blueprint & Use Case Portfolio V1**<br>A document detailing the successful integration roadmap of the CYberSynchrony modules within the organisation's infrastructure. Alongside, the portfolio will present tailored use cases that precisely resonate with CYberSynchrony objectives, ensuring a holistic and robust approach towards fortifying CYberSynchrony cyber defence mechanisms. | Chapter 3 | Provides the integration roadmap, high-level architecture, overview of components, and the methodologies adopted to deploy the platform's components in a scalable and resilient manner. |
| **TASKS** | | | |
| T8.1 | CYberSynchrony Integration and Use Case planning | Chapter 4 | Defines the structured testing approach for validating the integration of CYberSynchrony within real-world scenarios. |
| T8.2 | UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare | Chapter 5 | Focuses on the application of CYberSynchrony tools within a healthcare setting, includes the system architecture, current security mechanisms, cybersecurity awareness status, KPIs, and scenario definitions. |
| T8.3 | UC2: CYberSynchrony-Powered Public Administration | Chapter 6 | Demonstrates the deployment of the platform within a public administration environment, discusses the system's architecture, critical assets, cybersecurity awareness, KPIs, and scenarios designed to enhance the resilience of municipal services. |
| T8.4 | UC3: Fortifying Universities with CYberSynchrony | Chapter 7 | Describes the integration of CYberSynchrony modules in a university environment, details the architecture, assets, current security mechanisms, awareness levels, KPIs, and defined test scenarios. |

## 2.2 Linkage to other project outputs

Table 2 below explains how this deliverable is related to other project outputs and specific deliverables.

© CYberSynchorny, 2024

Table 2: Links to other Project Outputs/Work

| WP Number | Task Number | Deliverable Number related | Content |
|---|---|---|---|
| WP2 | T2.1, T2.2, T2.3, T2.4 | D2.1 | From D2.1, the general architecture and the high-level deployment architecture were obtained and analysed to understand the integration requirements of the components (tools), communication between them, and deployment locations. It formed the fundamental basis upon which the integration work was initiated.<br><br>Furthermore, the preliminary UC definitions, including roles within each UC, indicative scenarios, and requirements were taken and further extended in this deliverable for the full definitions and deployment requirements. |

## 2.3 Deliverable Structure

The deliverable is organised into distinct chapters to systematically present the integration approach, methodologies, and practical evaluations of the CYberSynchrony platform:

- **Chapter 1: Executive Summary**: Provides an overview of the deliverable's purpose, the main objectives of the integration blueprint, and the expected outcomes of the CYberSynchrony platform deployment.
- **Chapter 2: Introduction:** Introduces the CYberSynchrony project, its goals, and its significance in enhancing cybersecurity across different critical infrastructures. It also maps the project outputs and their linkage to this deliverable, setting the context for the integration blueprint and use case evaluations.
- **Chapter 3: Methodology for Integrating the CYberSynchrony Marketplace:** Discusses the integration roadmap, high-level architecture, and the methodologies adopted to deploy the platform's components in a scalable and resilient manner. This chapter also includes:
    - *Integration Roadmap:* Phased approach to implementing the platform.
    - *High-level Architecture Description:* Outlines the modular design across cloud, on-premise, and standalone layers.
    - *Definition of Tools and Relevance to Integration Work:* Maps each tool to its role in the CYberSynchrony ecosystem.
    - *Programming Languages and Technologies Used:* Explains the technologies and deployment strategies employed.
    - *Overview of Components (Tools):* Details the individual technologies and their deployment requirements.
- **Chapter 4: Methodology for Testing the CYberSynchrony Marketplace:** Defines the structured testing approach for validating the integration of CYberSynchrony within real-world scenarios. It includes the identification of roles, system architecture, and assets, as well as the planned testing methodologies to ensure reliability, compatibility, and cybersecurity readiness.

© CYberSynchorny, 2024

- **Chapter 5: UC1 – Demonstrating Comprehensive CyberHealth Security for Digital Healthcare (AMC):** Focuses on the application of CYberSynchrony tools within a healthcare setting, addressing the protection of Electronic Health Records (EHRs), telemedicine systems, and medical devices. It includes the system architecture, current security mechanisms, cybersecurity awareness status, KPIs, and scenario definitions.
- **Chapter 6: UC2 – CYberSynchrony-Powered Public Administration (EGL):** Demonstrates the deployment of the platform within a public administration environment, focusing on the MAESTRO platform used for incident management. It discusses the system's architecture, critical assets, cybersecurity awareness, KPIs, and scenarios designed to enhance the resilience of municipal services.
- **Chapter 7: UC3 – Fortifying Universities with CYberSynchrony (UPRC):** Describes the integration of CYberSynchrony modules in a university environment, focusing on protecting Learning Management Systems (LMS), student records, and administrative networks. This chapter details the architecture, assets, current security mechanisms, awareness levels, KPIs, and defined test scenarios.
- **Chapter 8: Conclusions:** Summarises the deliverable's findings, highlights the progress made in the integration of the platform, and outlines the next steps towards the final version of the integration blueprint (D8.4). It also reflects on the impact of the three use cases and the lessons learned during the integration process.

© CYberSynchorny, 2024

# 3 Methodology for Integrating the CYberSynchrony marketplace

Within WP8, the integration efforts are focused on unifying the components and mechanisms developed in WP3–WP6. These elements, defined by the technical and use case requirements analysis, framework architecture design, and technical specifications outlined in WP2, are assembled to create a cohesive system. The integration work in WP8, combined with the intuitive user interface to be developed in T6.1, culminates in the creation of the CYberSynchrony platform. This platform will enable users to access and purchase the individual modules of the Modular framework—thus transforming the platform into a fully functional CYberSynchrony Marketplace. A user-friendly interface featuring smooth navigation and engaging multimedia content (e.g., videos and quizzes) will be discussed further in the WP6 deliverables, ensuring diverse learning preferences are met and fostering a solid foundation in cybersecurity practices.

The CYberSynchrony platform incorporates advanced threat intelligence tools and analytics that provide superior threat assessment, robust risk monitoring, and prompt incident detection. Additionally, the platform facilitates cross-border collaboration through secure communication channels, supporting synchronised actions and efficient information exchange among Member States.

At its core, the CYberSynchrony platform is built around six core modules, that will be available for purchase through the marketplace. This modular design ensures flexibility and adaptability to meet varying cybersecurity demands. The functionalities of these modules are thoroughly detailed in the respective WP3–WP6 deliverables, while a brief summary is provided below:

- **CYRESCUE**: Enhances resilience by identifying vulnerabilities in critical systems and streamlining incident response. Automated tools and secure digital vaults protect systems and data, enabling rapid response to threats.

- **CYBERRA**: Focuses on real-time threat intelligence and tailored risk analysis for MS, ensuring reliable assessments through secure forensic methods.

- **CYBRITE**: Provides continuous monitoring to detect threats early. Advanced analytics support proactive risk management, minimising incident impact.

- **CROSS-CORE**: Facilitates secure, cross-border cooperation during cyber incidents. Blockchain technology ensures data integrity, enabling reliable information sharing among MS.

- **CYBERWISE**: Promotes cybersecurity awareness through engaging, educational tools, fostering a culture of cybersecurity across society.

- **CYBERGOPLUS**: Supports the implementation of robust cybersecurity policies and standards, ensuring consistent practices and regulatory compliance across sectors.

A high-level overview of the components and tools within these modules is provided in D2.1, with in-depth discussions available in the WP3–WP6 deliverables.

For platform deployment, a hybrid model combining cloud-based and on-premises solutions has been adopted. This approach enhances scalability, flexibility, and resilience, ensuring that the CYberSynchrony platform delivers robust cybersecurity measures in real-world environments. Moreover, all modules and their respective components are designed to be interoperable, forming the comprehensive CYberSynchrony platform.

In this chapter, the structured approach for integrating the CYberSynchrony marketplace is thoroughly discussed. First, the Integration Roadmap is presented, outlining the phased implementation strategy designed to seamlessly deploy the platform's components across various IT environments while ensuring scalability, resilience, and interoperability. Following this, the Integration Methodology introduces the high-level architecture of CYberSynchrony, detailing its modular design across cloud, on-premise, and standalone layers to support distributed processing and secure data exchange. In the Overview of Components (Tools) section, the deployment locations, interfaces, and communication protocols of each module are defined, followed by the Communication Interfaces and Data Exchange section, which details the necessary technical and environmental

© CYberSynchorny, 2024

configurations for successful integration. This structured approach ensures that all components are harmonised effectively, providing a solid foundation for the marketplace's testing and validation in real-world scenarios. Finally, the Programming Languages and Technologies Used highlights the technological stack, focusing on containerization, virtualization, and orchestration technologies to optimize deployment and maintainability.

## 3.1 Integration roadmap

The integration roadmap provides a structured framework that guides the systematic assembly of the CYberSynchrony marketplace. Integration, in this context, refers to the methodical process of interconnecting diverse cybersecurity modules, tools, and technologies to create a unified, efficient, and robust platform. This process is critical as it ensures that each individual component can communicate effectively, share data seamlessly, and function collectively to meet the project's overarching objectives in strengthening cyber defence mechanisms.

A well-defined integration roadmap is essential for several reasons. It establishes clear milestones and deliverables for technical teams, aligns the project's diverse work streams, and mitigates potential challenges by outlining specific steps from planning to final validation. This systematic approach not only enhances transparency during project execution but also ensures that the integrated platform is robust, scalable, and capable of addressing evolving cybersecurity demands.

The roadmap is composed of five key phases:

**Phase 1: Requirements, Architecture, and Module Specification**

In this initial phase, the focus is on gathering and analysing both functional and non-functional requirements, alongside technical specifications and architectural designs—building on the groundwork established in WP2 and D2.1. Key activities include:

- Gathering input from various stakeholders and, where applicable, third-party sources.
- Clarifying the specific functionalities and interfaces of each module, including inputs, outputs, and the expected data exchange.
- Defining communication channels, containerisation strategies, and the appropriate hosting environments for the modules.
- This phase lays the foundation for a coherent technical architecture and prepares the groundwork for subsequent design and integration activities spanning WP3 to WP6.

**Phase 2: Design and Documentation**

This phase transitions from planning to tangible design outputs. It involves:

- Creating mock-up designs of the CYberSynchrony Marketplace dashboard using design tools such as Figma.
- Developing detailed sequence diagrams and UML diagrams to visually represent module communications and data flow, as derived from the initial architectural designs in WP2. This design documentation serves as an essential guide for ensuring that the envisioned integration accurately reflects the planned technical interactions and process flows.

**Phase 3: Graphical HMI Development**

User experience is pivotal for ensuring platform adoption and effectiveness. In this phase, the emphasis is on designing a graphical Human Machine Interface (HMI) that is both intuitive and user-friendly. Key aspects include:

© CYberSynchorny, 2024

- Designing a dashboard interface based on established Dashboard Design Principles to ensure optimal usability.
- Creating a visual presentation that facilitates easy navigation and clear interpretation of key metrics and system statuses.
- This phase, primarily aligned with WP6, ensures that the end-user interaction with the integrated platform is seamless and efficient.

**Phase 4: Module Integration, Configuration, and Connectivity**

At this stage, the technical integration begins in earnest. The focus is on:

- Integrating the containerised CYberSynchrony modules into a unified system architecture.
- Configuring the integrated environment to ensure that all modules are properly connected and data exchange channels are functional.
- This phase consolidates the work from previous phases by technically assembling all components and establishing robust links among them, forming the operational backbone of the platform.

**Phase 5: Dashboard and Integration Testing**

The final phase is dedicated to rigorous testing and validation:

- Conducting comprehensive dashboard tests to ensure the user interface functions as intended.
- Performing integration tests to validate that all modules communicate successfully and that data flows as designed.
- This phase is critical for identifying and resolving any integration issues, ensuring that the final platform meets the defined performance criteria and stakeholder expectations.

The above phases are summarised in Figure 1 below. In summary, this integration roadmap outlines a clear, step-by-step process from requirements gathering and design through to full-scale integration and testing. By following these phases, the project is well-positioned to deliver a fully integrated CYberSynchrony platform that meets both technical and operational goals, ultimately enhancing the organization's cybersecurity posture.

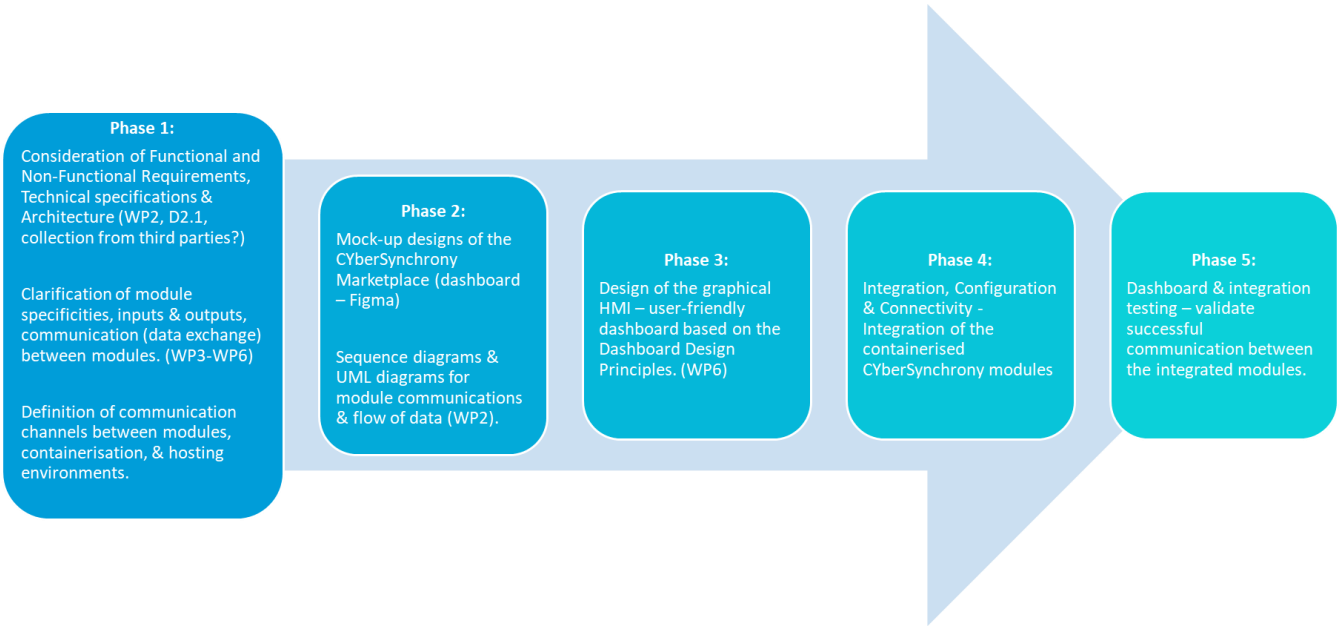


Figure 1: Integration roadmap of the CYberSynchrony Platform

© CYberSynchorny, 2024

## 3.2 Integration methodology

### 3.2.1 High-level architecture description

The CYberSynchrony platform is built as a modular, integrated cybersecurity framework that spans multiple deployment environments and enables interoperability across a wide range of tools developed in Work Packages 3, 4, and 5. Its architecture has been derived and incrementally refined from the baseline modular design presented in Deliverable D2.1 and is now instantiated as a deployment-aware blueprint, validated through Deliverables D3.1, D3.2, D4.1, D4.2, and D5.1.

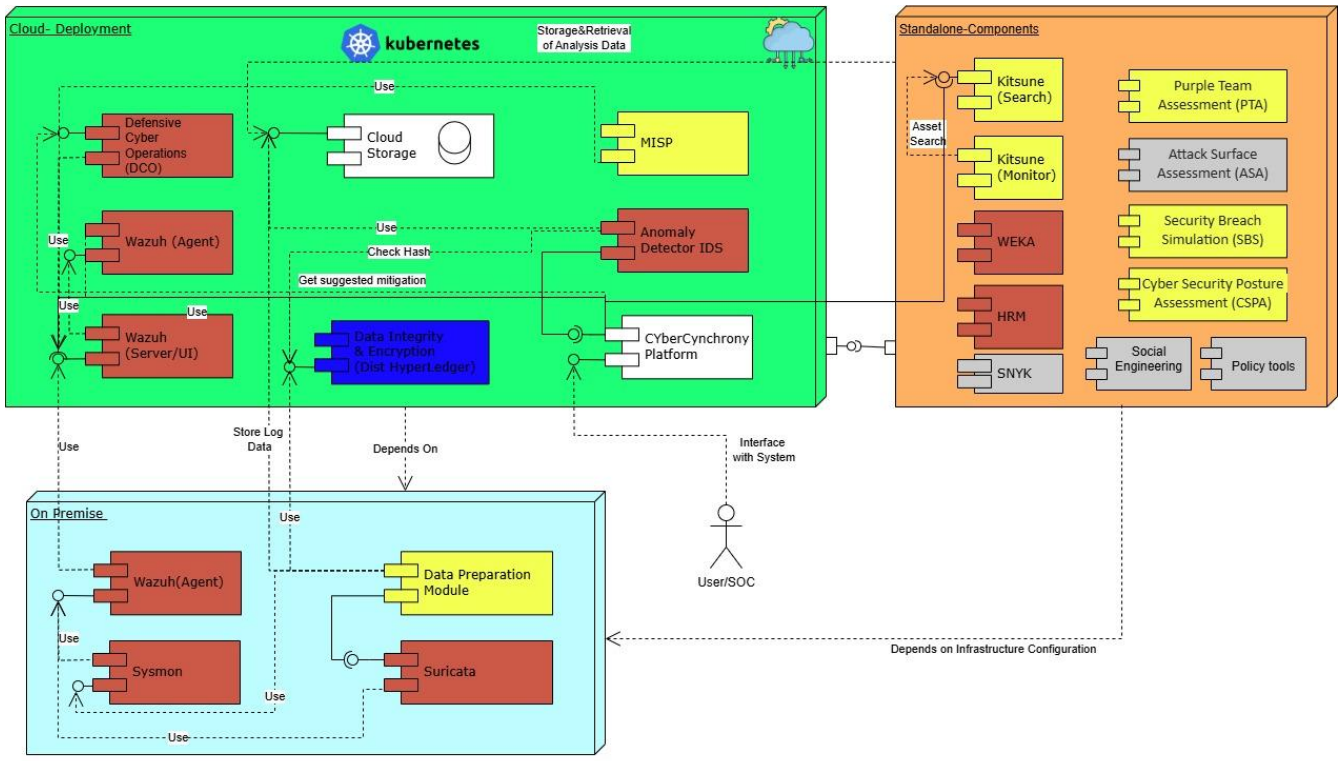


Figure 2: CYberSynchrony Deployment architecture

The architecture (Figure 2) consists of three main structural layers, as visualized in the color-coded system diagram:

- **Cloud Deployment Layer (Green):** Represents the platform's core runtime environment, hosted in a Kubernetes-managed cluster. This layer includes continuously running components such as the anomaly detection services, Wazuh server, Distributed ledger, defensive operation modules, and the core CYberSynchrony Platform itself.
- **On-Premise Deployment Layer (Light Blue):** Encompasses agents and data preparation components installed locally within organisations. These modules are responsible for collecting telemetry (e.g., system logs, network flows) and performing initial processing (e.g., hashing, transformation) before data is sent to the cloud.
- **Standalone Tools Layer (Orange):** Consists of components that are invoked on-demand and do not require continuous deployment. These are primarily used for post-analysis (e.g., forensic review, vulnerability scanning, risk profiling) and typically interact with the platform via the shared cloud storage layer.

At the centre of the architecture are two integral components, coloured in white:

- The **CYberSynchrony Platform and UI**, which acts as the central entry point and integration interface for all tools. It enables users to authenticate, launch modules, manage access, and interact with underlying services via Representational State Transfer (REST) Application Programming Interfaces (APIs) and web frontends.
- The **Cloud Storage**, which serves as the shared data hub for logs, alerts, forensic datasets, and processed results. It enables decoupled interaction between modules, allowing for scalable and asynchronous workflows.

**WP3: CYBERRA and CYRESCUE Module Integration (Yellow Components)**

WP3 delivers the threat intelligence and risk profiling capabilities of CYberSynchrony, through the CYBERRA and CYRESCUE modules. These tools, while primarily positioned in the standalone layer, play an active role in both upstream and downstream data workflows.

- **MISP**, deployed in the cloud, receives enriched log data and correlates it with known threats. It is fed by the Wazuh server and integrates CTI feeds into the system-wide analysis. The CYberSynchrony Platform serves as the access point to MISP functionality and CTI search features.
- **Kitsune Search/Monitor**, although lightweight and standalone, uses APIs to query threat metadata from storage or external intelligence sources. Users access it via the platform UI to perform asset-specific threat queries or link detections to known vulnerabilities.
- The **Risk Scenario Toolkit** interacts mainly with data stored in the Cloud Storage. After log batches or monitoring data are uploaded from on-premise agents and validated by the ledger (via WP5), the toolkit allows users to simulate breach impact, evaluate asset exposure, and generate resilience scores.

Collectively, WP3 modules consume input from WP4 (via logs and behaviour detection) and WP5 (via verified data streams), while publishing their outputs back into the platform for strategic use.

**WP4: CYBRITE Module Integration (Red Components)**

WP4 forms the operational core of the platform, implemented through the CYBRITE module. These components span the cloud, on-premise, and standalone layers and are central to runtime monitoring and detection.

- **Sysmon** and **Suricata**, deployed locally, feed system and network telemetry into the **Wazuh Agent**, which forwards them to the **Wazuh Server** in the cloud. This flow forms the foundation of the monitoring stack.
- The **Anomaly Detector IDS** uses logs collected from Wazuh/Suricata and accesses them from Cloud Storage. Before processing any log batch, it queries the Distributed Ledger Technology (**DLT)** to validate integrity (WP5). Only verified logs are used for AI-driven temporal anomaly detection.
- The DCO is activated upon detection events. It consumes input from IDS/UEBA modules and pushes automated policy actions via APIs. These actions include blocking IPs, revoking credentials, or triggering escalation workflows—reflected and recorded by the platform UI.
- Tools like **WEKA** and **HRM**, operate independently but access verified logs from storage. These tools support retrospective forensics, vulnerability discovery, and report generation, feeding back into the platform through manual uploads or API connectors.

Together, WP4 components establish a bi-directional data flow—from raw telemetry to alerts and response—and interface with both WP3 for intelligence enrichment and WP5 for verification and evidence handling.

**WP5: CROSS-CORE Module Integration (Blue Components)**

WP 5 provides the trust infrastructure of CYberSynchrony through the CROSS-CORE module. These components are responsible for ensuring data integrity, traceability, and secure exchange across the architecture.

© CYberSynchorny, 2024

- The **Data Preparation Module**, deployed on-premise, creates hashes (SHA-256) of log batches before uploading them to storage. It simultaneously registers these hashes on the **Distributed Ledger (Hyperledger Fabric)**.
- The **DLT** acts as a decentralised trust layer, allowing downstream modules (e.g., Anomaly Detector, forensic tools) to verify the authenticity of log files before analysis. This ensures that only validated data is processed or acted upon.
- **Cloud Storage** hosts the validated log batches and intermediate results. It is accessed by the CYberSynchrony Platform, detection systems, risk analysis tools, and post-forensic components.

The CROSS-CORE mechanisms are seamlessly embedded across the platform: WP4 and WP3 rely on WP5 to verify the integrity of every dataset they operate on. Moreover, WP5 guarantees that all sensitive data exchanges are logged, auditable, and compliant with project-wide privacy and trust policies.

**WP6: CYBERWISE and CYBERGOPLUS (Gray Components)**

The components associated with WP6, which include CYBERWISE (awareness and training) and CYBERGOPLUS (compliance and standardisation), are shown in grey in the deployment diagram. These include policy tools, social engineering modules, and training support environments. Their integration will begin in upcoming project phase considering that the WP6 starts at M12 and will further enrich the platform with human-centric, regulatory-aligned capabilities.

### 3.2.2 Definition of tools and relevance to the integration work

As part of the CYberSynchrony platform integration activities, IANUS created the Technical Plan Table (Figure 3) to systematically capture all necessary technical, operational, and deployment characteristics of each tool, service, or methodology participating in the project. The main goal of this structured approach was to centralise technical knowledge across partners, streamline integration efforts, and anticipate interoperability challenges early in the project. By capturing detailed information about each component—including its functionality, input/output data flows, deployment models, API availability, and use case relevance—we ensure that integration between modules is efficient, traceable, and aligned with the architecture envisioned in D2.1 and later on in D2.2 respectively. This approach not only facilitates better tool matching (*e.g., deciding how MISP correlates with Wazuh and Suricata*) but also reduces technical risks during the actual system assembly phase in WP8. Table 3 provides an explanation of the information collected for each tool, and its significance for the integration work.

Table 3: Explanation of the collected fields of the Technical Plan excel file

| Field | Explanation and Importance |
|---|---|
| **No.** | Unique identifier for each tool; helps in consistent referencing across deliverables. |
| **Tool/Service/Methodology** | Name of the tool being integrated (e.g., Wazuh, Suricata, MISP). |
| **Module** | Indicates which CYberSynchrony module the tool belongs to (e.g., CYBRITE, CYRESCUE). |
| **Task** | Refers to the specific task within the project (e.g., T3.1, T4.1) responsible for the tool's delivery and integration. |
| **Deliverable** | States in which deliverable the tool is formally documented, linking back to project outputs. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Functionality** | A short description of what the tool does; essential for identifying overlaps, gaps, and complementarities between tools. |
| **Partner** | The consortium member responsible for the tool; critical for defining roles during integration and testing. |
| **Type (Open Source, Commercial)** | Clarifies licensing and cost implications; open-source tools are easier to adapt and integrate without procurement barriers. |
| **TRL level** | Technology Readiness Level; helps assess maturity and integration readiness. |
| **Input Data** | Types of data that the tool requires for operation; essential for planning data pipelines and compatibility checks. |
| **Output Data** | Types of data the tool produces; important for downstream processing and interoperability with other components. |
| **Can it be containerized (Docker)?** | Indicates if the tool supports Docker deployment; essential for standardising deployment across the hybrid architecture. |
| **Deployment Requirements** | Lists any special hardware, OS, or network requirements if Docker is not available. |
| **Does this technology have an API?** | Shows whether the tool can be automated or integrated via APIs. |
| **If an API exists, specify the format (e.g., REST, SOAP)** | Specifies communication protocols needed for integration. |
| **Format of data exchanged (JSON, XML, CSV, etc.)** | Standardises data formats across the platform to ensure smooth ingestion and analysis. |
| **Does it have UI?** | Clarifies whether the tool has a user interface that must be exposed in the final CYberSynchrony Marketplace or SOC platform. |
| **Use Case Involved** | Indicates which pilot or use case the tool will support (e.g., Healthcare, Public Administration). |
| **Additional Notes** | Captures miscellaneous but important details such as AI/ML capabilities, federation options, security features, or known limitations. |

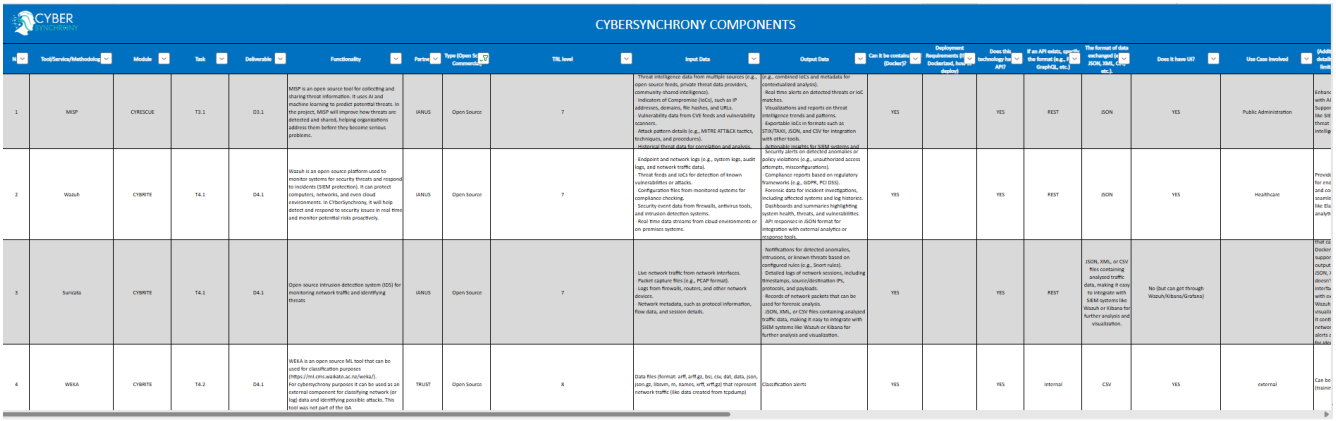


Figure 3: Technical Plan excel file

This approach is critical to the success of CYberSynchrony as it ensures integration readiness by allowing each partner to clearly understand how their tools are expected to interact with others. It guarantees architecture consistency by aligning real-world deployments with the logical and communication frameworks established in D2.1. By identifying potential incompatibilities, data format mismatches, or integration gaps early in the process,

it serves as a proactive risk mitigation measure, significantly reducing the chances of delays during testing or deployment. Furthermore, it enhances efficiency by minimising rework through the early alignment of functionalities and interface specifications. The method also promotes transparency and accountability by clearly mapping each tool to its responsible partner and integration pathway. Lastly, it fosters standardisation across the project by encouraging the adoption of containerisation and orchestration practices (e.g., Docker, Kubernetes), which simplifies deployment, scalability, and maintenance across the hybrid architecture.

## 3.3 Overview of Components (Tools)

This section provides a comprehensive overview of the individual components and tools that make up the CYberSynchrony platform. Each tool is described based on its deployment location, primary function, and integration within the broader architecture. The categorisation is structured to highlight the roles of cloud-based, on-premise, and standalone tools, emphasizing how they contribute to the platform's overall cybersecurity capabilities. This detailed mapping ensures that each component's technical specifications and interaction points are clearly defined, facilitating a seamless integration process. Additionally, the communication interfaces between these tools are outlined to illustrate data flow and interoperability across the different layers of the CYberSynchrony architecture. The information is presented in Table 4.

Table 4: Tools overview: deployment location and component interfaces

| Tool | Deployment Location | Component Interfaces |
|---|---|---|
| MISP | Cloud | Receives structured threat data from Wazuh; exports enriched threat intel to CyberSynchrony Platform via REST API (JSON format) |
| Wazuh | Hybrid (On-Premise + Cloud) | On-prem agent collects system logs → data prep → cloud agent retrieves from Cloud Storage → Server/UI processes and visualizes. Integrates with Suricata, Sysmon, MISP, CyberSynchrony Platform (JSON via REST API) |
| Suricata | On-Premise | Feeds EVE JSON alerts to the Data Preparation Module; correlated with Wazuh (via log ingestion) and further processed for threat analysis in the cloud |
| WEKA | External | CSV |
| SNYK | External | JSON |
| Human RM (HRM) | External | N/A |
| Anomaly Detector IDS | Cloud | Pulls validated logs from Cloud Storage; queries Blockchain Integrity Validator before processing; sends results to CYberSynchrony Platform (JSON via REST). |

© CYberSynchorny, 2024

| | | |
|---|---|---|
| Blockchain Integrity Validator | Cloud | Receives SHA-256 hashes from Data Prep Module; exposes verification service for all downstream components (REST API, JSON format). |
| Kitsune Monitoring | External | API Rest |
| Kitsune Search | External | API Rest |
| Attack Surface Assessment (ASA) | Internal | N/A |
| Purple Team Assessment (PTA) | Commercial and opensource combination | Agents to end users |
| SecurityBreachSimulation (SBS) | Internal | Agents in some cases |
| Defensive Cyber Operations (DCO) | Internal | Agents in some cases |

### 3.3.1 Communication Interfaces and Data Exchange

This subsection outlines the communication mechanisms and data exchange protocols between the various CYberSynchrony components. Understanding how these tools interact is critical for ensuring seamless integration, secure data flows, and effective threat detection across the platform. The communication mapping specifies the data flow direction—whether a tool sends, receives, or exchanges data—and the type of interface used for these interactions, such as REST APIs, gRPC, WebSocket protocols, etc. This structured representation, available in Annex I: Tools communication matrix, serves as a reference for understanding the interdependencies and real-time communication paths that enable the synchronisation of threat intelligence, incident response, and monitoring activities across CYberSynchrony modules. The matrix follows the colour coding established in the deployment architecture (Figure 2).

Additionally, Table 5 is organised to provide clear insights into how each tool interacts within the architecture, the types of data exchanged, and the integration points critical for maintaining secure and efficient operations. This overview serves as a reference for understanding how the platform components collaborate, enhancing transparency and facilitating troubleshooting during deployment and testing phases.

Table 5: Description of data exchanged between the tools

| Interaction | Data Description & Format |
|---|---|
| **Suricata → Data Prep Module** | EVE JSON logs (alerts, protocol metadata, flow data). Format: **JSON**, internal log forwarding. |
| **Data Prep Module → Cloud Storage** | Validated and enriched logs from Suricata, Wazuh, and Sysmon. Format: **JSON**, internal service call. |
| **Cloud Storage → Wazuh Agent (Cloud)** | Pre-validated logs. Format: **JSON**, pulled via scheduled data fetching routine. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Wazuh Agent → Wazuh Server/UI (Cloud)** | Telemetry data (endpoint logs, rule-based alerts). Format: **JSON**, internal event channel. |
| **Wazuh Server → MISP** | Sends selected alerts to MISP for enrichment. Format: **JSON**, via **REST API**. |
| **MISP → Wazuh Server/UI** | Sends enriched threat intelligence (IoCs, TTPs) for alert correlation. Format: **JSON**, via **REST API**. |
| **MISP → CYberSynchrony Platform** | Pushes correlated threat intel for user-facing dashboards. Format: **JSON**, **REST API**. |
| **Wazuh Server → CYberSynchrony Platform** | Shares log insights, incident alerts, and health status. Format: **JSON**, REST/Socket API. |
| **Sysmon → Data Prep Module** | Sends host-level process and telemetry data. Format: **EVTX converted to JSON**, local service pipeline. |
| **Suricata → Wazuh (Indirect via Data Prep)** | Alerts enriched and forwarded into Wazuh's log ingestion. Format: **JSON**, internal pipeline. |
| **Distributed Ledger → AI Anomaly Detector** | DLT queried to verify SHA-256 hash of incoming log batch before analysis. Format: JSON, REST API call and validation response. |
| **Data Prep Module → Distributed Ledger** | Submits SHA-256 hash of each log batch with timestamp and source ID. Format: JSON, REST API to Hyperledger Fabric endpoint. |
| **Cloud Storage → AI Anomaly Detector** | Provides access to verified log batches for temporal anomaly detection. Format: JSON log files, accessed via internal storage API. |
| **AI Anomaly Detector → CYberSynchrony Platform** | Pushes detected anomalies, alerts, and risk scores to the platform dashboard. Format: JSON, via REST or WebSocket API. |

## 3.4 Programming Languages and Technologies Used

In the context of CYberSynchrony's hybrid, modular architecture, effective deployment and orchestration technologies are vital for ensuring system scalability, portability, and operational resilience. This section introduces and contrasts three core technologies—Virtual Machines (VMs), Docker containers, and Kubernetes—highlighting their roles in the platform's DevOps lifecycle.

**Traditional Deployment and the Shift to Containers**

Historically, application deployment followed a "one application per server" model, leading to significant resource waste and operational overhead. Even with the introduction of virtualisation, resource duplication and dependency conflicts remained common. Scaling required provisioning multiple servers with the same configuration, often leading to version mismatches and inefficient infrastructure use.

Containers emerged to address these challenges by packaging applications and their dependencies in isolated, lightweight units that can run consistently across different environments. Unlike virtual machines, containers do not require a full guest OS, making them more efficient and quicker to deploy.

© CYberSynchorny, 2024

### Virtual Machines (VMs)

VMs emulate entire operating systems on a host through a hypervisor, offering robust isolation between environments. This makes them suitable for running legacy applications or systems requiring full OS-level separation. However, their resource intensity and slower boot times can be drawbacks for modern, scalable deployments. [1]

Key characteristics:

- Full Operating System (OS) emulation with strong isolation
- Resource-heavy and slower start-up
- Best suited for legacy or high-security scenarios

### Docker Containers

Docker containers are application packages bundled with all necessary dependencies, sharing the host OS kernel. This makes them more lightweight and efficient than VMs. They are ideal for microservices-based architectures, enabling reproducible environments and rapid scaling. [2]

Key characteristics:

- Lightweight, fast, and portable
- Share host OS kernel (less isolated than VMs)
- Ideal for Continuous Integration (CI)/ Continuous Deployment (CD) workflows and microservices

### Kubernetes (K8s)

Kubernetes is an open-source orchestration platform designed to manage containerised applications at scale. While Docker focuses on container creation and runtime, Kubernetes handles deployment automation, self-healing, load balancing, and scaling. It abstracts infrastructure complexity, ensuring high availability and fault tolerance across distributed clusters. [3]

Core benefits:

- Manages clusters of containers
- Automates scaling, rollouts, and recovery
- Cloud-agnostic and extensible via Application Programming Interfaces (APIs) and plugins

Table 6 below summarises the key characteristics of virtual machines, docker containers, and Kubernetes.

Table 6: Comparison of virtual machines, docker containers, and Kubernetes

| Feature | Virtual Machines (VMs) | Docker Containers | Kubernetes |
|---|---|---|---|
| **Resource Efficiency** | High overhead (full OS emulation) | Lightweight, shares host OS kernel | Dynamic resource allocation |
| **Isolation** | Strong OS-level isolation | Process-level isolation | Orchestrates but does not isolate |
| **Portability** | Slower to migrate | Highly portable | Enhances portability via orchestration |
| **Best Use Case** | Legacy systems or high-security | Microservices, lightweight workloads | Scalable production environments |

© CYberSynchorny, 2024

The decision on which of these technologies to employ for specific components is guided by the functional requirements of each module, the deployment context (e.g., cloud vs. on-premise), and constraints such as resource availability, performance, and security. For instance, Virtual Machines may be appropriate for legacy tools or environments requiring full OS-level isolation, while Docker containers enable efficient, lightweight deployment of modular services with minimal overhead. Kubernetes, in particular, is aligned with CYberSynchrony's platform-level needs due to its orchestration capabilities, automatic scaling, fault tolerance, and support for hybrid cloud strategies. Given the platform's goals of cross-organisational integration, real-time responsiveness, and modular interoperability, Kubernetes provides the infrastructure foundation necessary to ensure resilient operation, seamless integration across modules, and efficient resource management in a production-grade environment.

### 3.4.1 Architecture of Kubernetes

Kubernetes follows a two-tiered architecture comprising a **control plane** and **worker nodes**, each with distinct responsibilities. The Kubernetes architecture is visualised in

Figure 4 (a). The control plane governs the overall state of the cluster. Its core components include the **API Server**, which provides the main entry point for administrative commands; **etc**, a distributed key-value store that holds the cluster's configuration and status; the **Scheduler**, which assigns workloads (Pods) to available nodes based on defined policies (

Figure 4 (b)); and the **Controller Manager**, which ensures the system's actual state matches the declared desired state.

Worker nodes are the execution environments for running containers. Each node runs a **kubelet**, which ensures that containers are running according to their specifications; a **kube-proxy**, which manages network traffic between Pods and services; and a **container runtime** such as Docker or containerd.

At the core of Kubernetes workloads is the **Pod**—the smallest deployable unit in the system. A Pod may contain one or more tightly coupled containers that share the same network namespace and storage volumes, typically running related services. [4][5]

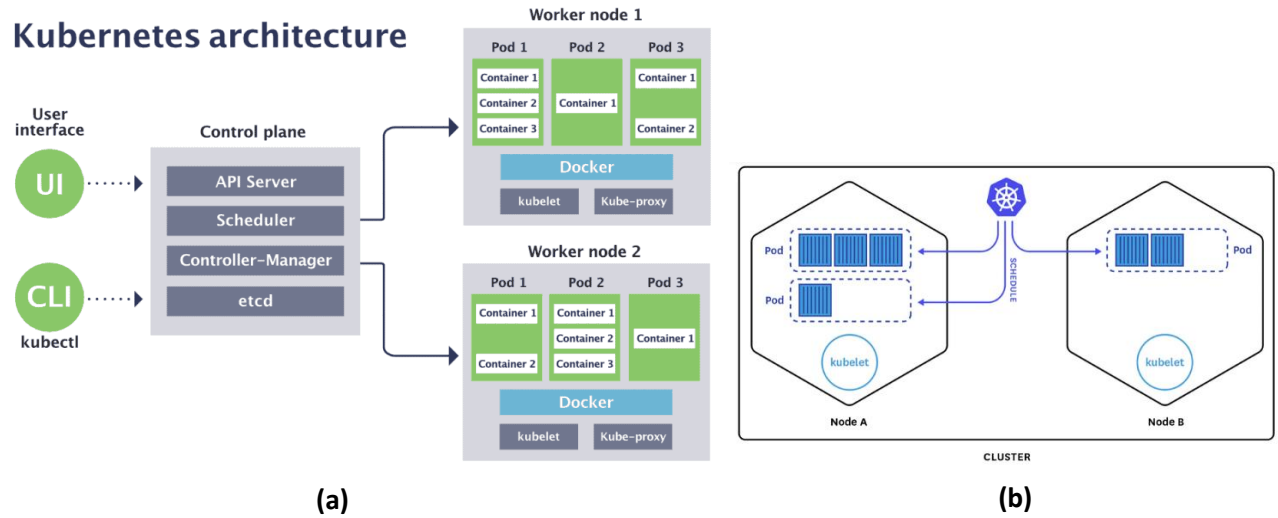


Figure 4: (a) Kubernete's architecture, visualising the different components and interactions, (b) Sheduler assigning pods to available nods

### 3.4.2 Integration and Interoperability in Kubernetes

Beyond container orchestration, Kubernetes offers a rich set of integration capabilities that are essential for managing complex application ecosystems like CYberSynchrony. It is inherently cloud-agnostic, supporting deployment on public cloud services, private data centres, and hybrid architectures. This flexibility allows CYberSynchrony to tailor deployments to each pilot's regulatory, performance, or data sovereignty needs.

Kubernetes integrates seamlessly with **CI/CD pipelines**, enabling automated application testing, deployment, and rollback. Tools such as Jenkins, GitLab CI, and Argo CD are widely used in conjunction with Kubernetes to streamline development workflows.

Observability is another critical integration domain. Kubernetes supports real-time monitoring and centralised logging through tools like Prometheus (for metrics), the ELK Stack (Elasticsearch, Logstash, and Kibana), and Fluentd, which can aggregate logs across distributed services.

Security integration is equally robust. Kubernetes implements Role-Based Access Control (RBAC) to manage user permissions, Network Policies to control inter-Pod communication, and Secrets Management for storing sensitive credentials. These features are vital for ensuring that the CYberSynchrony platform meets high standards of operational security. [6]

**Advanced Integration: Extensibility and Service Meshes**

Kubernetes is highly extensible through its API and custom resource definitions (CRDs). These allow developers to add domain-specific functionalities, such as custom controllers or automated workflows known as Operators.

To manage increasingly complex microservice communication patterns, Kubernetes can integrate with Service Meshes like Istio or Linkerd. These tools manage service-to-service traffic, enforce security policies, and provide advanced observability, all without requiring changes to application code. [7]

**Multi-Cluster and Hybrid Deployments**

For large-scale implementations like CYberSynchrony, Kubernetes enables multi-cluster deployments and federated management. This supports use cases where modules are deployed across multiple geographic regions or administrative domains. Kubernetes Federation simplifies cluster coordination, while hybrid deployments allow components to span cloud and on-premise infrastructures, balancing performance, cost, and compliance.

### 3.4.3 Frontend–Backend Integration Methodologies

As web applications grow more complex and interconnected, effective integration between the frontend (user interface) and backend (data and logic layer) becomes increasingly critical. In the context of the CYberSynchrony platform—where modular tools, real-time insights, and secure data flows are essential—choosing the right integration strategy ensures scalability, responsiveness, and interoperability across organisational environments.

Full-stack developers play a key role in implementing these integrations, but the technologies and patterns used must align with performance expectations, architectural decisions, and user needs. This section outlines the most commonly used frontend–backend integration methodologies, evaluates their respective strengths and trade-offs, and contextualizes their suitability within CYberSynchrony's hybrid deployment landscape.

**RESTful APIs**

Representational State Transfer (REST) is one of the most widely adopted paradigms for frontend–backend communication. It uses stateless HTTP operations (e.g., GET, POST, PUT, DELETE) to perform Create, Read, Update, and Delete (CRUD) actions on resources identified by unique URIs. [8]

REST APIs are language-agnostic, highly cacheable, and benefit from extensive tooling and community support. However, REST can suffer from over-fetching or under-fetching of data, especially in complex user interfaces that require multiple API calls to assemble all necessary data.

© CYberSynchorny, 2024

**GraphQL**

GraphQL provides a flexible alternative to REST by allowing clients to request exactly the data they need. It operates over a single endpoint and uses a strongly typed schema to define data structures, reducing over-fetching and improving performance. [9]

GraphQL excels in frontend-heavy applications with dynamic data needs, such as dashboards. However, it introduces complexity in caching, and the learning curve may be steep for teams unfamiliar with schema design and resolvers.

**gRPC**

gRPC is a high-performance Remote Procedure Call (RPC) framework developed by Google that uses Protocol Buffers (Protobuf) for efficient data serialization and HTTP/2 for transport. It is especially well-suited for internal communication between microservices due to its support for streaming, bi-directional communication, and strong typing.

Despite its performance advantages, gRPC lacks native browser support and often requires client stubs and additional tooling for web integration. This makes it more appropriate for backend-to-backend communications within distributed systems. [10]

**WebSockets**

WebSockets provide a persistent, full-duplex communication channel between the client and server, enabling real-time bidirectional data exchange. They are particularly useful in scenarios like cybersecurity dashboards, live notifications, or incident alerts, where updates must be reflected immediately without polling.

However, WebSocket-based architectures can present scalability challenges and require more careful state and connection management than traditional HTTP-based APIs. [11]

**Server-Sent Events (SSE)**

SSE offers a lightweight way for servers to push real-time updates to browsers over standard HTTP/1.1. It's useful for applications needing live data without the complexity of WebSockets but is limited to one-way communication from server to client.

SSE can be advantageous in simpler use cases, such as streaming alert messages or data feeds. However, browser support is inconsistent, and it is less suitable for interactive or bidirectional applications.

**Backend Integration Trade-Offs**

Each backend communication method presents trade-offs in terms of performance, complexity, real-time support, and ecosystem compatibility. In a modular system like CYberSynchrony, the choice of integration methodology may vary depending on the functionality and deployment context of each component. REST or GraphQL may be preferred for public-facing APIs, while gRPC or WebSockets may be better suited for internal module-to-module interactions where low latency and streaming are essential.

Table 7 provides a comparison of key features of integration methodologies.

Table 7: Comparison of integration methodologies

| Criteria | REST API | GraphQL | gRPC | WebSockets | SSE |
|---|---|---|---|---|---|
| Performance | Moderate | High | Very High | High | Moderate |
| Flexibility | Low | Very High | Medium | Medium | Low |

© CYberSynchorny, 2024

| | | | | | |
|---|---|---|---|---|---|
| Real-time Capability | No | With Subscriptions | Yes (Streaming) | Excellent | One-way Only |
| Ease of Use | High | Moderate | Low | Moderate | High |
| Tooling Support | Extensive | Growing | Advanced (Backend) | Good | Basic |

The choice of frontend–backend integration methodologies within CYberSynchrony is critical to achieving interoperability, responsiveness, and modular cohesion across its diverse tools and services. The selection depends heavily on the specific case. These methodologies not only ensure functional connectivity but also shape the user experience, scalability, and maintainability of the platform. As CYberSynchrony integrates tools from multiple partners with varying technologies and interfaces, a careful and context-aware application of these integration strategies will be key to ensuring seamless communication, consistent data flow, and robust platform performance across sectors and domains. Ultimately, no single methodology suffices for all cases. Integration strategies must be selected in conjunction with architectural requirements, performance expectations, and the nature of each tool within the CYberSynchrony ecosystem. Likewise, deployment strategies—whether based on Docker, Kubernetes, or VMs—will influence and constrain integration choices, depending on factors like resource availability, security requirements, and compatibility with legacy systems.

© CYberSynchorny, 2024

# 4 Methodology for Testing the CYberSynchrony marketplace

The demonstration and evaluation activities under WP8 are dedicated to validating the CYberSynchrony platform and ensuring it meets a broad range of end-user cybersecurity needs—particularly in the areas of threat awareness and training. The primary objective is to unlock the platform's full operational potential by rigorously testing its functionalities within real-world environments.

Validation, demonstration, and evaluation efforts focus on three key sectors that correspond to the project's designated use cases:

- **UC1:** Demonstrating Comprehensive CyberHealth Security for Digital Healthcare
- **UC2:** CYberSynchrony-Powered Public Administration
- **UC3:** Fortifying Universities with CYberSynchrony

The execution plan for these use cases adopts a phased approach to gradually develop and roll out the CYberSynchrony ecosystem. In each use case scenario, the platform will be integrated into the organisation's infrastructure and then assessed against defined end-user expectations, organizational needs, and practical application scenarios. Based on feedback from initial prototypes and performance assessments, iterative enhancements will be implemented to refine the platform components continuously.

Furthermore, the use case portfolio illustrates how each scenario aligns with CYberSynchrony's core objectives while providing a comprehensive integration plan. This plan ensures system compatibility and proactively identifies potential integration challenges or vulnerabilities during testing. [12][13]

A detailed testing and validation methodology is also presented, linking each use case's objectives to specific KPIs. This methodology identifies the platform modules that will undergo testing and outlines targeted test scenarios designed to rigorously evaluate the system's performance. The sections that follow describe this comprehensive testing approach, while the detailed use case portfolios—presented in Chapters 5, 6, and 7—demonstrate how each use case aligns with the overall testing plan.

## 4.1 Testing Methodology

The testing and validation methodology is composed of several key elements that must be identified and executed within the three testing environments. These elements form the backbone of a successful evaluation process for the CYberSynchrony platform. The following sections detail each element, highlighting its relevance and contribution to the overall testing strategy.

**Use Case Needs and Motivation:**

Understanding the specific needs and motivations of each use case is critical for tailoring the testing process. This component outlines the background information of each use case, describing the particular challenges and requirements of the sector involved. It explains why a robust cybersecurity platform is necessary to address these challenges, building upon the foundational needs analysis provided in D2.1. By clearly identifying these needs, the testing plan can be aligned with real-world operational conditions, ensuring that the evaluation accurately reflects the environment in which the CYberSynchrony platform will operate.

**Roles and Responsibilities:**

Clear definition of roles and responsibilities is essential for the coordination of the testing effort. This component identifies the various stakeholders who contribute to the validation process, such as IT specialists, end-users, security analysts, and training personnel. Examples of groups and defined duties may include:

- **IT Specialists:** Focus on technical integration, system performance, and ensuring data flow integrity.
- **End-Users and Employees:** Provide practical feedback on usability and training effectiveness.

© CYberSynchorny, 2024

- **Security Analysts:** Monitor the impact on cybersecurity defences and identify potential vulnerabilities.
- **Training Coordinators:** Evaluate the effectiveness of cybersecurity awareness initiatives. Establishing these roles ensures that every participant knows their specific responsibilities, facilitating a structured and efficient testing process.

**System Architecture and Assets Identification:**

A comprehensive understanding of the system architecture and thorough identification of key assets in each use case environment are essential for ensuring successful integration of the CYberSynchrony platform. This phase involves mapping out the entire technological landscape of the use case, which provides the foundation for a smooth and efficient integration process.

Asset identification is critical because it enables project teams to pinpoint all components that will interact with the CYberSynchrony platform. This includes identifying core systems—the central technological pillars that drive operations—as well as the supporting subsystems. Equally important is documenting the network topology, which details how these systems are interconnected, the dependencies between them, and the typical data flow paths. Such a detailed layout allows for a clear understanding of where and how the CYberSynchrony modules can be best integrated.

Furthermore, specifying the testing environment is crucial. Whether the assessment is performed in a live operational setting or a dedicated testing sandbox will influence the integration approach. A live environment offers insights into real-world performance and immediate impact on existing systems, while a controlled environment allows for isolated testing, reducing risk during the initial rollout.

In essence, a detailed mapping of the system architecture and asset identification accomplishes several key objectives:

- **Ensures Compatibility:** It maps out how the CYberSynchrony components align with the existing infrastructure, helping to identify potential conflicts or compatibility issues before full deployment.
- **Identifies Integration Challenges:** By understanding the current state of systems and networks, the team can foresee and pre-emptively address any challenges or vulnerabilities that might arise during integration.
- **Tailors Test Scenarios:** Detailed asset identification enables the design of test scenarios that are specific to the organisational setup, ensuring that validation efforts are relevant and impactful.
- **Optimizes Security:** It provides a basis for verifying that the integration of new modules will complement existing security measures, thereby safeguarding the organisation against potential threats.
- **Streamlines Deployment:** A clear architectural roadmap facilitates an organised and phased integration process, reducing downtime and ensuring a smooth transition.

**Current Security Mechanisms:**

Documenting current security mechanisms in place within each use case is important for establishing a baseline for comparison. This component involves a thorough inventory of the existing cybersecurity tools, protocols, and processes before the integration of the CYberSynchrony platform. Understanding the baseline security posture serves multiple purposes:

- It helps identify any compatibility issues between current mechanisms and the new platform components.
- It provides a benchmark against which improvements can be measured post-implementation.
- It offers insights into potential areas where the integration might further strengthen the overall security framework.

**Cybersecurity Awareness Programmes:**

© CYberSynchorny, 2024

Assessing the existing cybersecurity awareness programmes within each use case is essential for tailoring the training aspects of the CYberSynchrony platform. This component should detail:

- Whether current awareness initiatives exist.
- The target audiences (e.g., general employees, C-level executives, IT or cybersecurity professionals).
- The tools and methodologies currently used for training.
- The different proficiency levels or tailored programmes available based on user roles. Analysing these factors allows the integration of customised training modules that address any gaps in awareness and ensure that the training interventions are well-suited to the needs and proficiency levels of the intended audience.

**Use Case Objectives and KPIs:**

The objectives and key performance indicators (KPIs) for each use case, as specified in the grant agreement, serve as the benchmark for testing the platform. These metrics provide clear targets and measurable outcomes that reflect the broader goals of the project. This component:

- Guides the selection of specific CYberSynchrony tools and modules for evaluation.
- Forms the basis for designing targeted test scenarios.
- Enables the objective measurement of improvements in cybersecurity performance post-integration. By aligning testing activities with these established objectives and KPIs, stakeholders can accurately assess the impact of the platform on the operational environment.

**Scenario Definition:**

The scenario definition is the preliminary formulation of specific test scenarios that will be conducted across the three use case environments. Each scenario is designed to evaluate the functionality and effectiveness of the CYberSynchrony platform relative to the defined KPIs. A comprehensive test scenario includes the following elements:

- **Scenario Description:** A detailed narrative outlining the purpose and context of the test.
- **Assumptions & Pre-Conditions:** A list of prerequisites and conditions that must be met before the test can begin.
- **Goal (Successful End Condition):** The desired outcome that indicates test success.
- **Involved Actors:** Identification of roles and stakeholders responsible for executing the test, based on the defined responsibilities.
- **Scenario Initiation and Main Flow:** A sequence of steps detailing how the test will be executed, data collected, and KPIs assessed.
- **Evaluation Criteria:** Specific benchmarks or target values derived from the KPIs against which the test outcomes will be measured.
- **Tools and Validation:** The tools and methods that will be used to execute the test and validate the results. This detailed definition ensures that every test scenario is methodically planned, allowing for systematic execution and precise evaluation of the platform's performance.

By addressing each of these components within the testing methodology, the evaluation process is designed to be thorough, coherent, and directly aligned with the project's objectives. This structured approach not only facilitates a comprehensive understanding of the platform's performance but also ensures continuous refinement and improvement based on measurable outcomes. In the use case portfolio, Chapter 5, 6, and 7, the UCs provide an initial identification of these critical elements that serve as the foundation for kick-starting the preparations for the implementation of the testing phase.

© CYberSynchorny, 2024

# 5 UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare

## 5.1 Use Case information

Use case 1 focuses on enhancing of cybersecurity in Digital Healthcare and is led by the CYberSyncrony partner Apostolos Loucas Medical Center (AMC), the largest and most comprehensive outpatient medical centre in Cyprus. Over time, technology has increasingly become an integral part in healthcare with imaging machines such as X-rays, CT scans, MRIs or ultrasounds storing results digitally, simplifying evaluation, sharing, and storage. That evolution has also significantly affected Apostolos Loucas Medical Centre (AMC). As increasingly more sensitive data is stored digitally, hospitals, clinics, and research institutions increasingly have become a prime target for cyberattacks. The reliance on legacy IT infrastructure, which often lacks modern security mechanisms, makes these organisations vulnerable to cyber threats. Furthermore, the rise of telemedicine, cloud-based healthcare systems, and AI-powered diagnostics has expanded the attack surface for cybercriminals. [14]

Critical areas in healthcare that require cyber protection:

1. **Electronic Health Records (EHR/EMR):**
   Breaches can lead to data loss, manipulation, or unavailability, directly impacting patient care and safety.
2. **Appointment and Telemedicine Systems:**
   Cyberattacks on scheduling or virtual care platforms can disrupt service delivery and delay medical assessments.
3. **Internal Communication & Network Systems (Emails, VoIP, Intranet):**
   Unauthorised access to communications may result in data leaks or internal misinformation.
4. **Financial and Billing Systems:**
   These systems contain sensitive payment, insurance, and billing information and are prime targets for fraud and ransomware.
5. **Reputation and Public Trust:**
   A cyberattack can severely damage the centre's credibility, leading to patient mistrust and potential legal consequences.
6. **Guest and Staff Wi-Fi Networks:**
   Unsecured or poorly segmented networks can act as entry points for attackers into the core system.
   Key challenges driving the need for this use case:

1. **Ransomware & Data Breaches:** Healthcare data is valuable and often targeted by cybercriminals.
2. **Vulnerabilities in Medical Devices:** Many Internet of Medical Things (IoMT) devices lack security measures, making them easy targets for attackers.
3. **Regulatory Compliance:** Organisations must comply with the General Data Protection Regulation (GDPR), Network and Information Security Directive (NIS2) Directive, and Digital Operational Resilience Act (DORA) Directive.
4. **Insider Threats & Human Errors:** Healthcare staff often lack cybersecurity awareness.
5. **Integration of Security Solutions:** There is a need for seamless detection, response, and mitigation of cyber threats.

By addressing these needs the cybersecurity in healthcare will be enhanced, the incident detection and response time will be reduced, minimising or even eliminating the damage of cyber-attacks and the secure handling of patient information will be always ensured.

© CYberSynchorny, 2024

AMC is going to provide a real Digital Healthcare environment to be tested and evaluated within the CyberSyncrony platform and its functionalities.

UC1 aligns with CYberSyncrony's objectives by implementing and testing its key components in a real-word healthcare environment. By utilising **CYRESCUE** for penetration testing, **CYBERRA** & **CYBRITE** to monitor and assess the risks and incidents, **CROSS-CORE** to securely exchange healthcare data, **CYBERWISE** to train medical staff and **CYBERGOPLUS** for compliance and security audits we will effectively protect our healthcare facility from cyber threats and provide valuable insights for future cybersecurity deployments across the healthcare sector.

The roles and responsibilities within UC1 are shown in Table 8.

Table 8: Roles and Responsibilities within UC1

| Role | Responsibility in Testing and Evaluation |
|---|---|
| IT Staff | Deploy and configure CYberSyncrony security tools, security testing, Monitor the system and incident response |
| Medical Doctors, Nurses and secretaries | Test the usability, reporting any delays or disruptions caused by security controls, participate in cybersecurity training. |
| Management | Oversee the implementation and effectiveness of applied measures, ensuring that security protocols align with hospital operations and regulatory compliance, and making strategic decisions based on testing outcomes to enhance the hospital's overall cyber resilience and risk management policies. |

## 5.2 System Architecture and Assets Identification

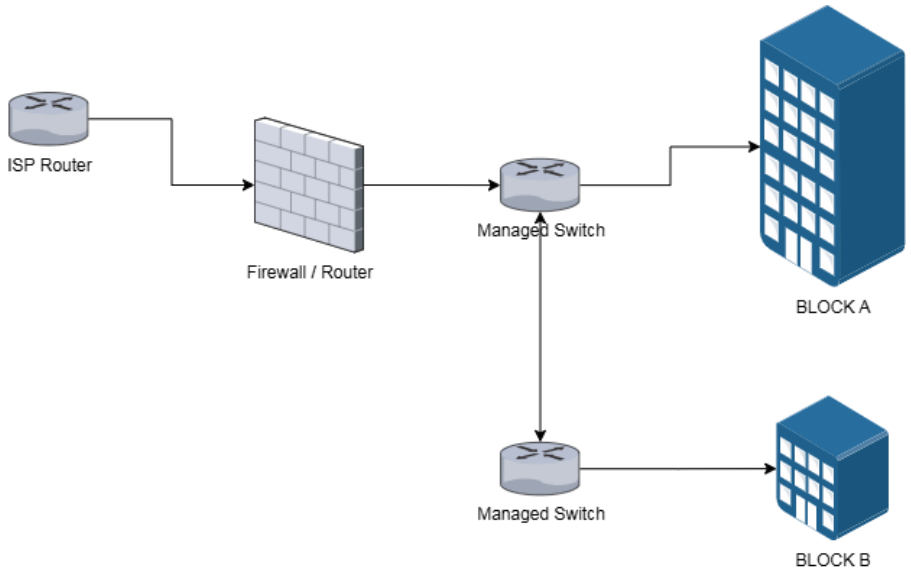


Figure 5: Healthcare Infrastructure – External

Our healthcare facility is divided in Block A and Block B, each designed to serve different departments and functions (Figure 5).

© CYberSynchorny, 2024

Block A houses the Radiology Department, a Call Centre and reception areas on each floor. It also includes Doctors' Offices, exam rooms, Management Offices and a Small Operating Room. Block B contains the Chem Lab, reception areas on each floor, Doctors' Offices, exam rooms and a Small Operating Room.

A MicroTik router acts as the gateway to the internet, providing an entry point for all external communication. The router typically connects to the internet service provider (ISP) and routes traffic between your local network and the outside world.

Then the internal network is distributed on each block and each floor by managed switches with advanced features, allowing greater control over data flow within our network. The internal network of the Healthcare facility is segmented into different zones with the use of Virtual Local Area Networks (VLANs) as shown in Figure 6.

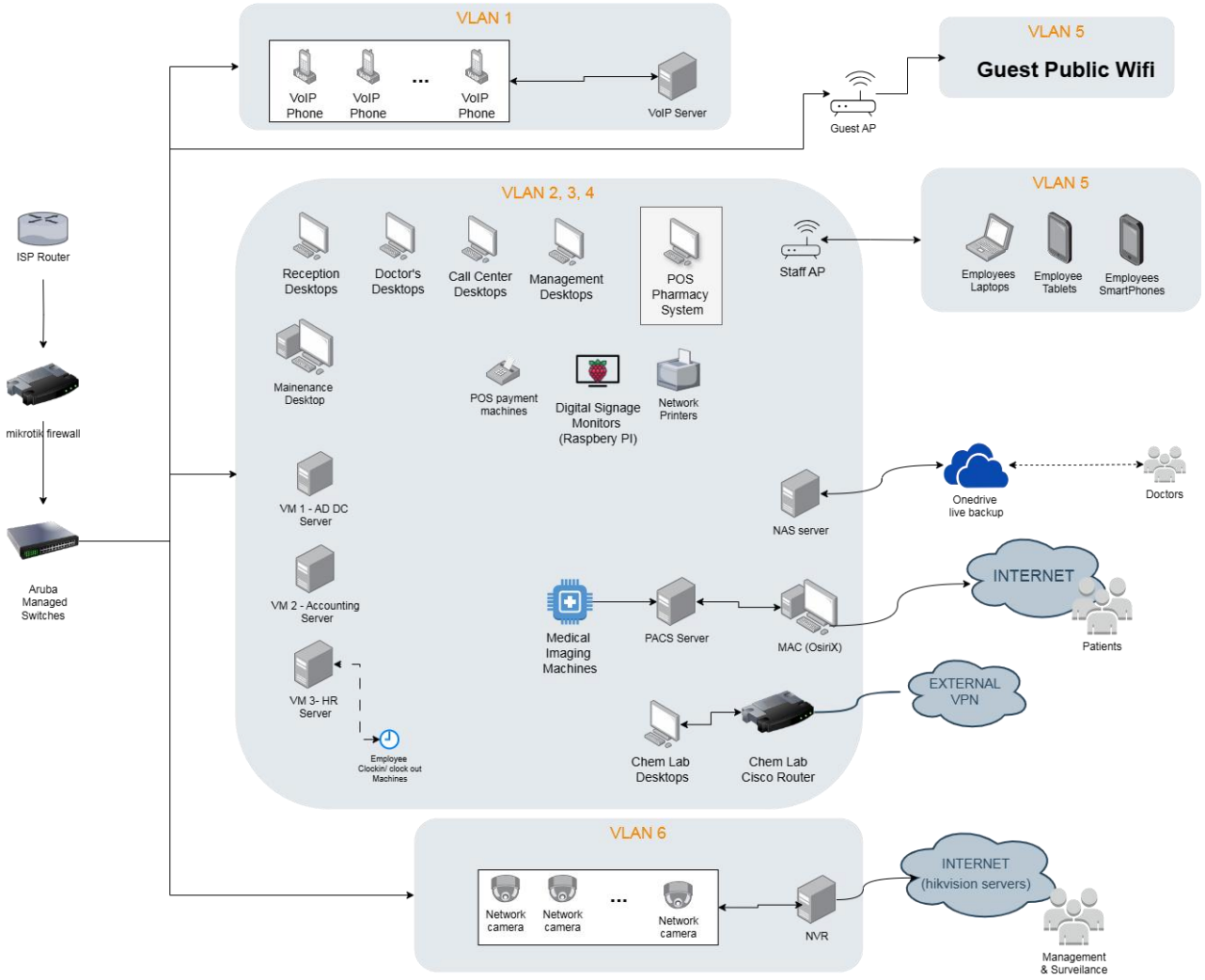


Figure 6: Healthcare Infrastructure – Internal

To ensure network isolation and avoid unauthorized access, the network is split into different VLANs (Virtual Local Area Networks), each dedicated to specific devices and user groups.

**VLAN 1 – VOIP Server and Phones:** This VLAN is dedicated to the VOIP system, including the VOIP server and Internet Protocol (IP) phones.

**VLAN 2, VLAN 3, VLAN 4 – Computers, Printers, and Other Network Devices:** These VLANs are designated for the various devices used within the medical facility. Devices like computers, printers, and other network devices

© CYberSynchorny, 2024

in both Block A and Block B are grouped into separate VLANs to isolate them from other devices. These VLANs are intended solely for use by AMC employees, such as secretaries, doctors, and management staff.

**VLAN 5 – AMC Employees' Wireless Devices:** This VLAN is allocated for wireless devices used by AMC employees, such as laptops, smartphones, and tablets. This ensures that wireless devices, which are more vulnerable to security threats, do not have direct access to critical resources in other VLANs. It also allows for easier management of wireless access, ensuring proper allocation of bandwidth and network resources.

**VLAN 6 – Network Cameras, NVRs, and DVRs:** This VLAN is dedicated to network cameras, Network Video Recorders (NVRs), and Digital Video Recorders (DVRs). These devices are essential for surveillance and security purposes. We have to be certain that the video traffic generated by cameras does not interfere with other network traffic and the video streams must be secured. The NVRs and DVRs have access to the Internet and can be accessed remotely by using dedicated applications with user accounts.

**VLAN 7 – APs Dedicated to Guest Internet Access:** This VLAN is designed specifically for Access Points (APs) that provide internet access to guests. Devices connected to this VLAN are only allowed to access the internet, with no access to internal network resources. This separation ensures that guest devices, which may not have strong security measures, cannot access sensitive or critical systems within the organization. It also improves overall network performance by isolating guest traffic from the internal network.

AMC's core systems that hold the majority of critical data essential to the smooth operation of the facility are:

1. **Storage Equipment – NAS (Network attached storage)**

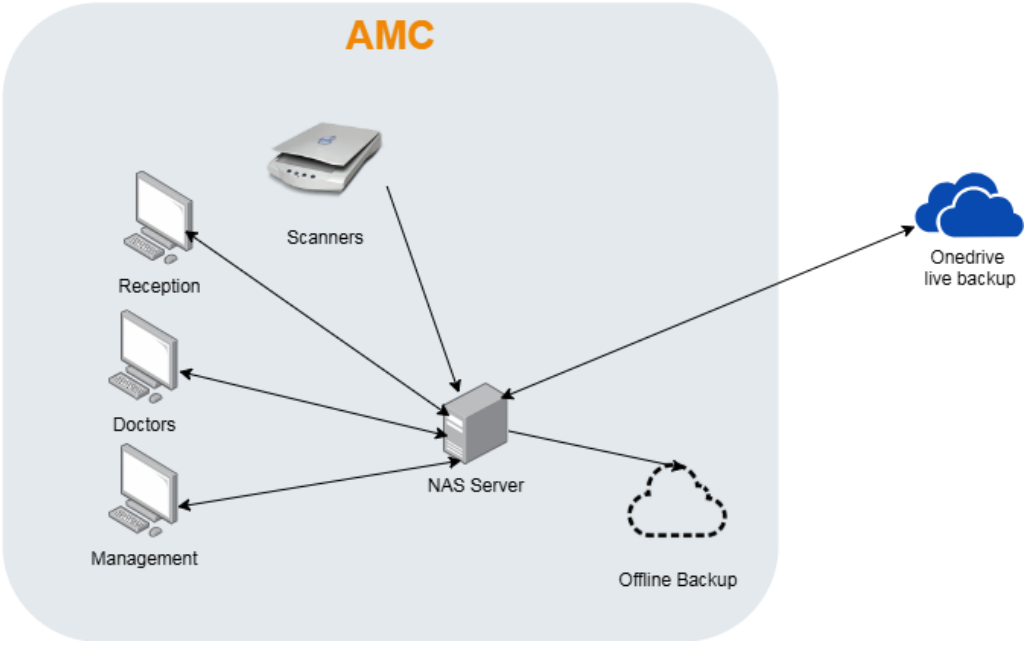


Figure 7: Storage Equipment – NAS

The Synology Server acts as the central Network-Attached Storage (NAS) server for AMC (Figure 7) storing the majority of the facility's files and ensuring centralised, secure access to critical data. Below is a more comprehensive overview of the system:

- **Role-Based Access Control (RBAC)**: employees' access to files and folders is determined by their specific roles within the organization. For example, secretaries may only have access to administrative documents, while doctors may have access to patient records or clinical data.

© CYberSynchorny, 2024

- **Online Bidirectional Backup to OneDrive**: To safeguard against data loss, the NAS is set up with an online bidirectional backup to OneDrive, ensuring that all files stored on the NAS are automatically backed up to the cloud. The bidirectional nature of the backup means that if files are modified on the NAS or in OneDrive, changes are synced between both locations, ensuring that the latest versions are always accessible and protected. This also helps prevent data loss in the event of hardware failure or accidental deletion, providing an additional layer of data redundancy.
- **Restricted Access – On-Premises Access Only**: NAS access is restricted to the AMC buildings, meaning that only devices physically present within the facility's network can access the files stored on the NAS. Each employee has their own unique user account, which is required for authentication, ensuring that access to the NAS is tracked and controlled.
- **Remote Access Through OneDrive (on Special Occasions)**: Remote access to the NAS is highly restricted. On special occasions, such as during emergencies, remote access is granted via OneDrive for a limited time for limited files.
- **File Versioning and History**: This feature allows users to revert to previous versions of files, ensuring that if a file is accidentally modified or deleted, it can be restored to an earlier version. This is especially useful in environments like healthcare, where data integrity is critical, and a mistake or unauthorised change could have serious consequences. It also provides an audit trail, allowing users to track changes and determine who made edits to files and when.

2. **Storage Equipment – PACS**

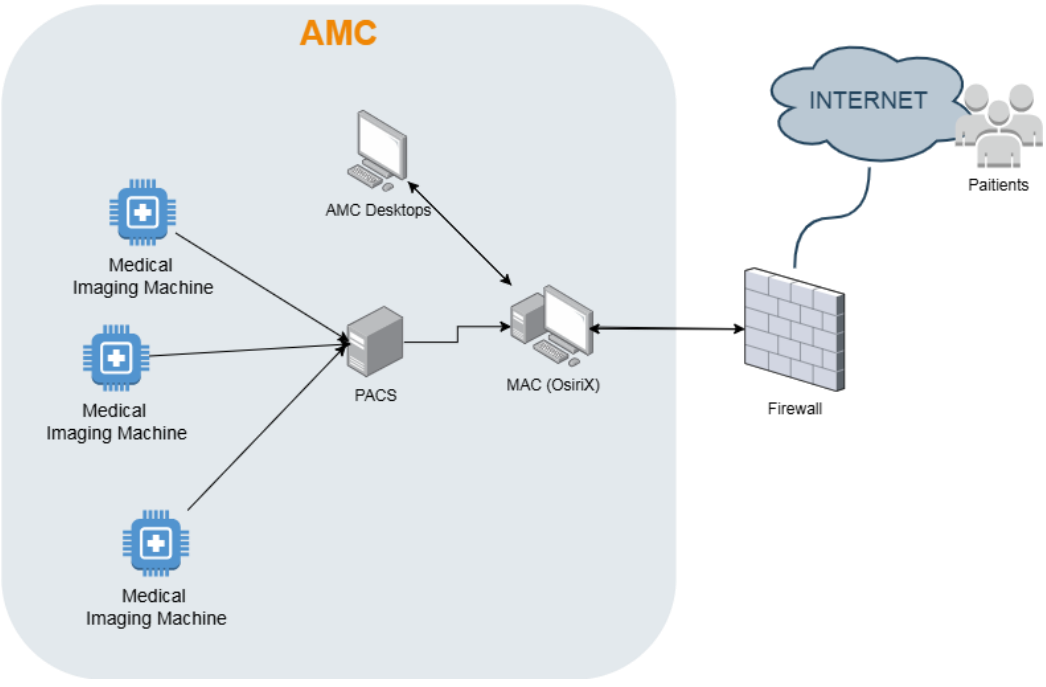


Figure 8: Storage Equipment – PACS

A Picture Archiving and Communication System (PACS), Figure 8, is a critical medical imaging technology used in healthcare to streamline the management of medical images. It allows for the digital storage, retrieval, sharing, and management of medical images, replacing the traditional film-based methods that were previously used. With PACS, healthcare providers can efficiently access, analyse, and share images, which enhances the speed and accuracy of diagnosis and treatment.

All medical imaging machines (such as X-ray, CT scans, MRIs, ultrasounds etc) are connected to the PACS server. These machines automatically send exam results directly to the PACS server, where they are stored digitally. This system holds all patient exam history, making it easier to retrieve previous imaging data and track changes over time for more accurate assessments.

A macOS computer running the OsiriX Application serves as the web server for the PACS system. OsiriX is a popular DICOM (Digital Imaging and Communications in Medicine) viewer and workflow solution that enables both internal and external access to the PACS data. This setup allows authorized users, such as doctors and radiologists, to securely access, view, and analyze the stored images from any location.

To further enhance the workflow, AMC employees upload doctor's reports related to the exams into the system. These reports are linked to the corresponding images in the PACS, ensuring that all relevant information is available in one place.

Additionally, patients can access their medical imaging data via the internet using a secure link. To ensure privacy and security, patients must log in with their credentials before being granted access to their images and associated reports. This system gives patients the convenience of reviewing their own medical data remotely, whether for personal reference or to share with other healthcare providers.

Table 9: UC1 assets description

| Asset Name | Description | Data processed by the asset | Criticality |
|---|---|---|---|
| Active Directory Server | Virtual Machine, windows server 2019, that acts as the Domain Controller and Print server in the AD Environment | All user accounts, groups, computers, OUs, and other AD objects, password hashes for authentication, GPOs and logon scripts, SIDs mapping for users, groups, and resources and users roaming profiles including users' files | High |
| PACS | Storage Server for medical imaging. | Medical Images and scans, patient information and metadata, DICOM data, Physician & Radiologist Reports, Audit & security logs | High |
| OsiriX | A mac OS pc that acts like a web server to share patients' exams through the web. | All data that is handled by the PACS | High |
| NAS Server | dedicated centralised storage device used for daily operations, management, and general-purpose storage | Administrative & financial data, research & compliance data, communication & collaboration data, patient data, doctor data, employees' data, and files | High |

- **Other Software:**
  - Sofia HR Human resource software platform,
  - Esoft accounting software
- **Other Platforms:**

© CYberSynchorny, 2024

- GESY - Cyprus' universal healthcare system providing comprehensive medical services to all permanent residents and Cypriot citizens,
- Google Workspace Platform – email, calendar

## 5.3 Current Security Mechanisms

The current security mechanisms within the UC1 infrastructure are shown in Table 10.

Table 10: List of UC1 security mechanisms.

| Name | Description |
|---|---|
| Network security | All different VLANs are isolated from each other, guests have no access to the internal infrastructure, strict rules are enforced on our firewalls and each machine has antivirus software installed. Unused services from the servers/pcs are stopped. |
| Restricted access | AD users do not have administrative rights to avoid installation of malicious software, complexity of passwords is enforced and passwords are periodically changed, access to assets outside of AMC internal infrastructure is limited, each account logs out automatically to prevent unauthorised access, default passwords are changed on all devices (printers, cameras, nvrs etc...) |
| Employees Training | Each employee receives basic cybersecurity training and frequent trainings and seminars are organized to educate employees |
| Endpoint Protection | Each endpoint has antivirus and internet security software installed, managed from a centralised platform configured with an overview of their health. Regular OS updates and patches. |
| Compliance & Standards | ISO 9001: Ensures consistent quality management and customer satisfaction.<br>ISO 14001: Promotes effective environmental management and sustainability.<br>ISO 45001: Enhances occupational health and safety in the workplace |

## 5.4 CYberSecurity Awareness Program

The status of current cybersecurity awareness in UC1 is described in Table 11.

Table 11: UC1 status of cybersecurity awareness

| Question | Answer |
|---|---|
| Does any cybersecurity program exist? | No |
| What is the target audience? (e.g., Generic employees, C-level, Cybersecurity/IT professionals) | None |
| What tools are utilised for awareness training? | None |

© CYberSynchorny, 2024

| | |
|---|---|
| How many proficiency levels exist? | None |
| Do different cybersecurity awareness programs exist based on the target audience? | No |

## 5.5 UC1 KPIs and Objectives

The KPIs for UC1, along with their target values and mapping to CYberSynchrony modules, are presented in Table 12. These KPIs serve as the benchmark for testing the platform. The objectives of UC1 and their mapping to the KPIs are detailed in Table 13.

Table 12: UC1 KPIs and target values

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

Table 13: UC1 Objectives and mapping to KPIs

| # | Objective | Related KPIs |
|---|---|---|
| UC1.O1 | Implementation robust encryption methods to secure sensitive patient data. | UC1.KPI1 |

© CYberSynchorny, 2024

| | | |
|---|---|---|
| UC1.O2 | Conduct regular cybersecurity audits and risk assessment of healthcare IT systems. | UC1.KPI3 |
| UC1.O3 | Establish a real-time monitoring system for detecting unauthorised activities and potential data breaches. | UC1.KPI4 |
| UC1.O4 | Develop and implement a comprehensive incident response plan for cybersecurity threats. | UC1.KPI4 |
| UC1.O5 | Train healthcare staff in cybersecurity best practises and awareness. | UC1.KPI2 |

***UC1.O1 Implementation of robust encryption methods to secure sensitive patient data.***

The implementation of robust encryption methods directly supports UC1.KPI1 (100% successful encryption implementation) by ensuring that all sensitive patient data, previously unprotected, is securely encrypted. This enhances compliance with GDPR, HIPAA, and NIS2, protecting electronic health records (EHRs) and hospital communications from unauthorised access.

To evaluate encryption effectiveness, CROSS-CORE ensures secure data exchange, while CYBERGOPLUS monitors compliance with regulatory requirements. Wazuh enforces encryption at endpoints, detecting unauthorised access attempts, and CYBERRA analyses risks related to encryption weaknesses. The evaluation process includes pre-implementation assessments to identify unencrypted data, real-time security monitoring post-implementation, and final audits to verify encryption success. Achieving these goals strengthens cybersecurity in digital healthcare, ensuring data integrity, regulatory compliance, and improved security resilience.

***UC1.O2 Conduct regular cybersecurity audits and risk assessment of healthcare IT systems.***

Regular cybersecurity audits and risk assessments in UC1 ensure compliance, threat mitigation, and security resilience in healthcare IT systems. This directly supports UC1.KPI3, which aims to increase audit frequency and achieve a 50% reduction in critical security findings. By conducting bi-annual audits and continuous risk assessments, the medical centre can proactively identify vulnerabilities, assess compliance with GDPR/NIS2, and improve overall cybersecurity posture.

To achieve these goals, CYBERGOPLUS will oversee compliance monitoring and regulatory reporting, while CYBERRA will conduct AI-driven threat intelligence and cyber risk analysis. Additionally, MISP will be used for threat intelligence sharing, ensuring that audit findings contribute to broader cybersecurity awareness. The evaluation process will involve pre-audit risk assessments, automated vulnerability scans, penetration testing, and post-audit reporting, verifying that security gaps are addressed efficiently and regulatory standards are met. By implementing these measures, UC1 enhances healthcare cybersecurity resilience, reduces risk exposure, and ensures continuous improvement in IT security operations.

***UC1.O3 Establish a real-time monitoring system for detecting unauthorized activities and potential data breaches.***

The implementation of a real-time monitoring system in UC1 is essential for early detection of unauthorised activities and potential data breaches, directly supporting UC1.KPI4 (60% reduction in detection and response

© CYberSynchorny, 2024

time). By continuously monitoring healthcare IT systems, medical devices, and patient data access, the system ensures proactive threat detection, preventing data breaches, ransomware attacks, and insider threats.

To achieve this, CYBRITE will be the primary tool real-time threat detection, analysing log data, user behaviours, and network traffic. CYBERRA will provide AI-driven risk analysis, identifying anomalies and suspicious activities, while Wazuh will enforce endpoint monitoring and detect potential intrusions. Evaluation will include real-time attack simulations, automated incident detection tests, and analysis of system logs, ensuring that security alerts are generated and responded to within the targeted timeframe. This approach strengthens cyber resilience in digital healthcare, minimising the risk of prolonged security incidents and ensuring regulatory compliance with GDPR, NIS2 and DORA.

***UC1.O4 Develop and implement a comprehensive incident response plan for cybersecurity threats.***

A comprehensive incident response plan ensures that cybersecurity threats are detected, contained, and mitigated efficiently, directly supporting UC1.KPI4 (60% reduction in detection and response time). By defining clear escalation procedures, automated response mechanisms, and post-incident recovery strategies, the IRP helps minimise downtime, data loss, and patient care disruptions in healthcare environments.

To achieve this, CYRESCUE will be used for penetration testing and attack simulations, assessing the effectiveness of response actions. CYBRITE will enable real-time monitoring and automated alerting, ensuring incidents are identified promptly. CYBERGOPLUS will oversee regulatory compliance in incident handling, ensuring that responses align with GDPR, NIS2, and DORA guidelines. Evaluation will involve simulated cyberattacks (ransomware, phishing, insider threats), response time analysis, and post-incident forensic assessments, ensuring that threats are contained and resolved within the target timeframe. This structured approach enhances cyber resilience in healthcare, preventing long-term disruptions and ensuring continuous improvement in security operations.

***UC1.O5 Train healthcare staff in cybersecurity best practices and awareness.***

Training healthcare staff in cybersecurity best practices and awareness directly aligns with UC1.KPI2 (Training in cybersecurity best practices) by enhancing the overall security posture and reducing the risk of breaches or incidents that could disrupt healthcare services. Trained staff can avoid or identify possible threats like phishing emails, suspicious activity and take appropriate action quickly. This reduces the time between identifying a potential attack and initiating the response, helping to mitigate damage. Also educating staff on proper handling, storage, and sharing of sensitive patient information ensures compliance with data protection regulations and minimises the risk of accidental data breaches. Additionally educating staff on creating strong, unique passwords and the importance of regularly updating them helps to secure access to systems and sensitive data.

To implement this CYBERWISE provides hands-on cybersecurity training, including phishing simulations and interactive learning modules, helping employees recognise and respond to threats. The HRM system ensures training participation is monitored, and certifications are tracked. Meanwhile, simulated cyberattacks and phishing tests measure real-world readiness, and an incident reporting system gathers data on security events to evaluate improvements over time.

## 5.6 Scenario Definition

The scenarios that will be conducted in UC1 to evaluate the functionality and effectiveness of the CYberSynchrony platform relative to the defined KPIs are shown below.

© CYberSynchorny, 2024

Table 14: UC1 Test Scenario 1

| Scenario name | UC1.KPI1 Data Encryption Implementation |
|---|---|
| **Description** | The healthcare organisation must improve security and compliance with industry regulation by ensuring that all sensitive healthcare and personal data is encrypted. |
| **Assumptions & Pre-Conditions** | Some healthcare systems currently lack encryption, systems will not experience downtime due to encryption implementation, Ability to integrate to current systems |
| **Goal (Successful End Condition)** | 100% of previously unencrypted systems successfully implement encryption. |
| **Involved Actors** | IT staff |
| **Scenario Initiation** | The IT staff initiates an encryption rollout across all unencrypted healthcare systems |
| **Main Flow** | 1. Identify systems without encryption<br>2. Select appropriate encryption standards<br>3. Apply encryption methodologies to databases, file storage and com channels<br>4. Conduct encryption testing and validation<br>5. Monitor system performance and security<br>6. Train relevant staff<br>7. Verify encryption implementation through audits |
| **Evaluation Criteria – Related KPIs** | Percentage of previously unencrypted systems that now have encryption - UC1.KPI1 |
| **Modules to be validated** | CROSS-CORE |

Table 15: UC1 Test Scenario 2

| Scenario name | UC1.KPI2 Training in cybersecurity best practices |
|---|---|
| **Description** | The healthcare organisation improves staff awareness of cybersecurity threats by training at least 30 healthcare professionals in best practices |
| **Assumptions & Pre-Conditions** | Healthcare staff currently have little or no cybersecurity training, A training program is available, Staff participation is mandatory or highly encouraged |
| **Goal (Successful End Condition)** | A minimum of 30 staff members complete the training. |
| **Involved Actors** | Employees, Healthcare staff (Nurses & doctors), Secretaries, IT staff |
| **Scenario Initiation** | A cybersecurity training program is scheduled and announced |
| **Main Flow** | 1. Identify staff members requiring training<br>2. Schedule training sessions |

© CYberSynchorny, 2024

| | |
|---|---|
| | 3. Deliver training on key topics (phishing, password management, secure data handling etc)<br>4. Evaluate participants' understanding through quizzes.<br>5. Record participation and completion rates.<br>6. Issue certificates or recognition to trained personnel. |
| **Evaluation Criteria – Related KPIs** | Number of staff trained - UC1.KPI2 |
| **Modules to be validated** | CYBERWISE |

Table 16: UC1 Test Scenario 3

| **Scenario name** | **UC1.KPI3 Audit Frequency & Reduction in Critical Findings** |
|---|---|
| **Description** | The healthcare organization enhances cybersecurity by increasing audit frequency and reducing critical security findings by 50% |
| **Assumptions & Pre-Conditions** | Current audits are conducted annually, Past audits identified multiple critical security findings, The CyberSynchrony module is deployed to improve compliance and security |
| **Goal (Successful End Condition)** | Bi-annual audits with a 50% reduction in critical security findings after one year. |
| **Involved Actors** | IT staff |
| **Scenario Initiation** | An updated audit schedule is created to conduct audits every six months. |
| **Main Flow** | 1. Schedule and perform the first post-implementation audit.<br>2. Identify and document security issues.<br>3. Implement CyberSynchrony module security improvements.<br>4. Conduct second audit after six months.<br>5. Compare critical findings with previous reports.<br>6. Implement further security enhancements as necessary. |
| **Evaluation Criteria – Related KPIs** | Frequency of audits, percentage of reduction in critical findings -UC1.KPI3 |
| **Modules to be validated** | CYBERRA, CROSS-CORE |

Table 17: UC1 Test Scenario 4

| **Scenario name** | **UC1.KPI4 Detection and Response time** |
|---|---|

© CYberSynchorny, 2024

| | |
|---|---|
| **Description** | The healthcare organisation continuously monitors their systems and networks for security incidents and alerts and implements a rapid response plan to quickly contain and mitigate potential incidents. |
| **Assumptions & Pre-Conditions** | Ability to integrate to current systems, Historical data on detection and response times is available, CyberSynchrony module is implemented for real-time monitoring |
| **Goal (Successful End Condition)** | A 60% reduction in incident detection and response time. |
| **Involved Actors** | Employees, Admin, IT |
| **Scenario Initiation** | Continuous process |
| **Main Flow** | 1. The internal network is continuously monitored with CyberSynchrony.<br>2. A security anomaly, unauthorised access attempts or unusual behaviour is detected<br>3. An alert is generated and sent to the IT who analyses and categorizes the threat.<br>4. Immediate remediation actions are taken.<br>5. Incident is documented and logged.<br>6. Post-incident review identifies areas for further improvement. |
| **Evaluation Criteria – Related KPIs** | Reduction in detection and response time compared to historical data |
| **Modules to be validated** | CYBRITE, CROSS-CORE |

© CYberSynchorny, 2024

# 6 UC2: CYberSynchrony-Powered Public Administration

## 6.1 Use Case information

Use Case 2 focuses on enhancing the cybersecurity posture of **MAESTRO**, an incident management platform used by the **Municipality of Egaleo (EGL)** to handle Municipal Police incidents and coordinate emergency management with improved efficiency and decreased response time. MAESTRO acts as a central nervous system during relevant events, enabling coordinated responses primarily of the Municipal Police but of multiple stakeholders as well, such as police, fire departments, emergency health services, and other municipal authorities.

While MAESTRO is not a cybersecurity solution in itself, its role as a **critical infrastructure asset** makes it a high-value target for cyber threats. A successful attack on this platform could lead to the disruption of essential public services, real-time decision-making paralysis, or even endanger citizen lives during emergencies.

This use case is implemented as part of **CYberSynchrony**, which aims to safeguard public administration through the integration of advanced cybersecurity technologies developed under the aforementioned project. [15]

### 6.1.1 Needs and Motivation

The motivation behind this use case stems from the **growing cyber threat landscape** affecting public administrations and critical municipal services. As the Municipality of Egaleo continues to digitize its operations and improve response coordination through platforms like MAESTRO, it faces several key challenges:

- **Operational Dependency on Digital Systems**: MAESTRO is integrated into the workflows of emergency and public safety services. A cyber incident affecting MAESTRO could halt or delay critical responses.
- **Lack of Resilience to Advanced Threats**: A plethora of cybersecurity mechanisms protecting MAESTRO have been already deployed, such as firewalls, and password-protected access controls. However, there is still room for improvement to create the best mix of tools that will help defend against modern, persistent threats.
- **Monitoring and Detection**: Real-time threat monitoring that supports advanced alerting or forensic analysis during or after a cyber event.
- **Human Error & Awareness Gaps**: Many operators and municipal employees have not received targeted cybersecurity training, increasing the likelihood of successful phishing attacks or accidental system misconfigurations.
- **Compliance and Data Integrity**: Given that MAESTRO handles sensitive data (e.g., incident logs, response coordination records), it must comply with strict data protection regulations and ensure the immutability of records, especially in legal or forensic contexts.

**Motivation Summary**: There is an acknowledged need to fortify MAESTRO against cyberattacks by integrating advanced security solutions, improving operator awareness, and ensuring business continuity during cyber events. This will help preserve citizen trust, protect critical services, and maintain operational integrity under threat.

### 6.1.2 Relevance to CyberSynchrony

This use case offers a **real-world validation scenario** for the integration and deployment of **CyberSynchrony modules** in a high-stakes public sector environment. It demonstrates how the platform's suite of tools can be effectively applied to **secure operational infrastructure** rather than purely digital services. The relevance of each CyberSynchrony module is outlined below:

- **CYRESCUE** (Digital Service Security):

© CYberSynchorny, 2024

Deployed to identify and mitigate vulnerabilities within the MAESTRO system, conduct penetration tests, and simulate denial-of-service or privilege escalation attacks to test resilience.

- **CYBERRA** (Identity Verification & Risk Assessment):

Used to audit and secure user access to MAESTRO through behavioural analysis and risk scoring. Supports the introduction of multi-factor authentication and risk-based access control policies.

- **CROSS-CORE** (Public Record Integrity via Blockchain):

Ensures that MAESTRO's critical records—such as dispatch logs, incident responses, and communication records—are tamper-resistant and cryptographically verifiable, supporting forensic readiness and legal compliance.

- **CYBRITE** (Incident Detection & Response):

Enables real-time monitoring of MAESTRO's infrastructure, detecting suspicious activity and automating response workflows to isolate threats without disrupting core emergency operations.

- **CYBERWISE** (Cybersecurity Awareness & Training):

Educates municipal employees and MAESTRO operators on cyber hygiene, phishing detection, and incident reporting. Customized training modules foster a proactive security culture and reduce human-related risk vectors.

By applying CyberSynchrony in this use case, the project demonstrates:

- **Real-world impact** in securing municipal critical infrastructure.
- **Modular adaptability** of the CyberSynchrony tools across diverse domains.
- **Public value creation**, as the protection of emergency services directly supports citizen safety, trust, and resilience in smart city operations.

This use case represents a unique opportunity to show how **CyberSynchrony enables municipalities to defend not only digital services but also mission-critical operational platforms that link the digital and physical world.**

The roles and responsibilities within UC2 are shown in Table 18.

Table 18: Roles and Responsibilities within UC2

| Role | Responsibility in Testing and Evaluation |
|---|---|
| CyberSecurity Analyst | Conducts tests to identify weak points in the MAESTRO platform. |
| Awareness trainer | Organises awareness sessions for MAESTRO users and municipality employees. |
| Project manager | Gathers results and prepares reports |

© CYberSynchorny, 2024

## 6.2 System Architecture and Assets Identification

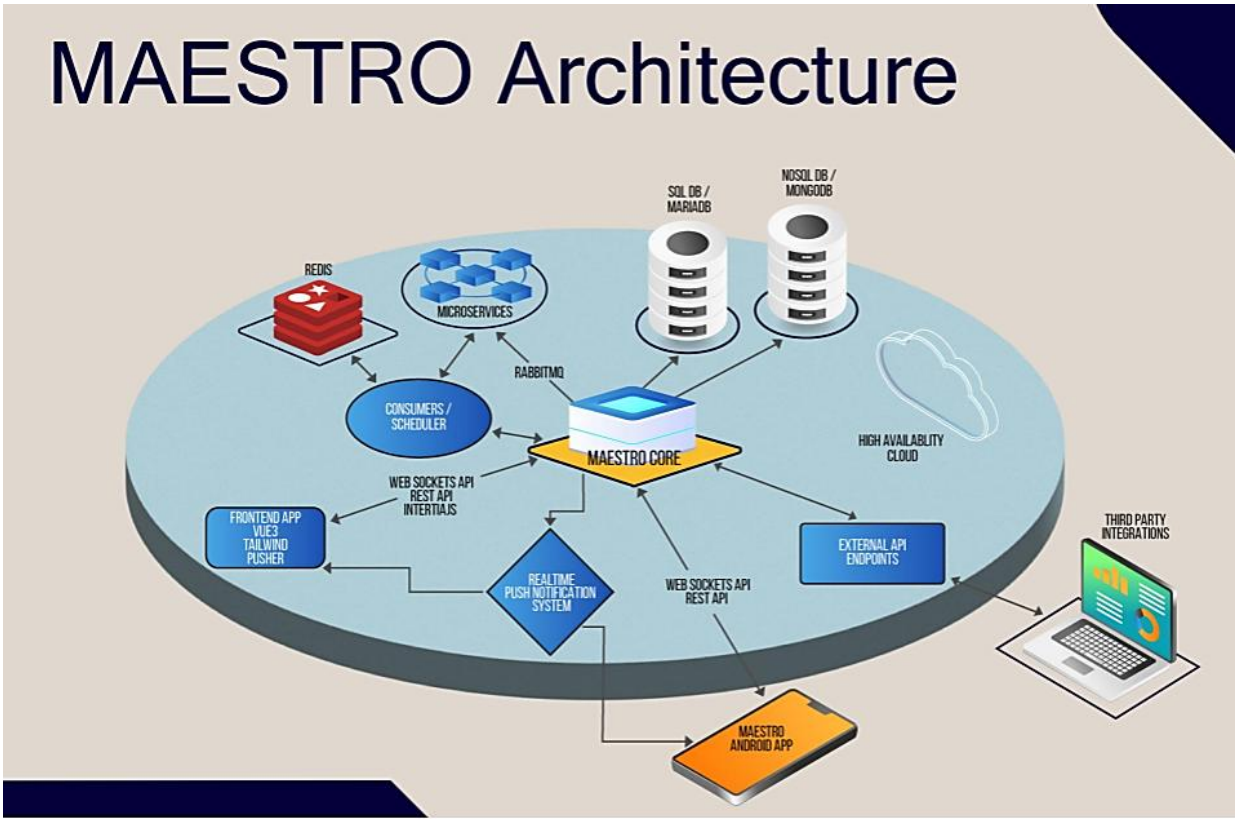


Figure 9: UC2 infrastructure architecture diagram

The MAESTRO architecture (Figure 9) is designed around a **centralised core system** that interacts with multiple supporting components including databases, microservices, APIs, and external integrations. The system is hosted in a **high-availability cloud environment**, making it scalable and resilient.

**1. MAESTRO Core (Central System)**

This is the heart of the platform. All critical functionalities flow through this core:

- It orchestrates data movement between services.
- It manages user interactions and external API calls.
- It communicates directly with internal and external components (like databases and microservices).
- It serves as the central hub for data processing, coordination, and real-time communication across the MAESTRO ecosystem.

**2. Consumers / Scheduler**

This component handles scheduled tasks and job queues. It:

- Consumes data from message queues (RabbitMQ).
- Triggers background processes or workflows (e.g., alert generation, report creation).
- Supports the orchestration of microservices.

**3. Microservices**

MAESTRO adopts a microservices architecture, meaning:

- Each core function (e.g., notifications, user authentication, data validation) runs as a self-contained service.

© CYberSynchorny, 2024

- These microservices communicate with the MAESTRO Core and with each other using APIs and RabbitMQ (a messaging broker).
- This makes the system modular, allowing easy updates or scaling of specific components without affecting the entire platform.

**4. RabbitMQ (Message Broker)**

RabbitMQ is responsible for asynchronous communication between components.

- When a user submits a request or data is received, RabbitMQ sends it to the appropriate service.
- It helps manage real-time workloads and system decoupling, increasing system performance and reliability.

**5. Databases**

There are two main types of databases integrated into MAESTRO:

a. Structured Query Language (SQL) Database (DB) (MariaDB):

- Stores structured data like user records, logs, event histories.
- Useful for transactional operations and relational queries.

b. NoSQL DB (MongoDB):

- Stores unstructured or semi-structured data, such as sensor feeds, message logs, or metadata.
- Ideal for performance and horizontal scaling.

**6. Redis**

Redis is an in-memory data store used for:

- Caching
- Session management
- Fast access to temporary data (e.g., alert queues)
- Helps improve system performance by reducing database load.

**7. Web Sockets API / REST API / InertiaJS**

MAESTRO supports both REST APIs and WebSocket APIs, enabling:

- Data retrieval and interaction from frontend apps.
- Real-time updates to clients (without refreshing the interface).

InertiaJS helps manage client-side routing and rendering.

**8. MAESTRO Android App**

- A mobile interface for field personnel (e.g., emergency responders, municipal agents).
- Receives real-time updates, tasks, and can send incident data back to the MAESTRO Core.

**9. Realtime Push Notification System**

- Sends instant notifications to users based on events.
- Works with both web and mobile interfaces.
- Helps in real-time emergency coordination, status updates, and alerts.

**10. External API Endpoints**

Enables integration with external systems:

- National services
- Geographic information systems
- Identity verification providers

© CYberSynchorny, 2024

Promotes interoperability and data exchange.

**11. Third-Party Integrations**

MAESTRO is designed to connect with third-party tools such as:

- Dashboards and analytics tools
- IoT platforms
- Other government systems

This allows it to be extended and customized according to specific municipality needs.

**12. High Availability Cloud**

The entire system is deployed in a high availability (HA) cloud infrastructure, ensuring:

- Resilience against failures
- Scalability to handle large loads
- Continuity during updates or maintenance

In this use case, the CyberSynchrony modules will be integrated as **defensive layers around MAESTRO**, not altering its core operations, but enhancing its protection, observability, and auditability.

## 6.3 Current Security Mechanisms

To keep data as safe as possible, **MAESTRO runs only on a private cloud**, meaning it is completely separate from the open internet. This separation makes it much harder for hackers or other outside threats to reach the system.

When people use MAESTRO's web application, their information is protected with Transport Layer Security (**TLS**) **encryption** (the same technology used by secure websites), which keeps data safe while it's being sent or received — making sure no one can spy on it or tamper with it.

For storing data, MAESTRO uses **strong encryption methods** to protect sensitive information in its databases:

- **MySQL and MariaDB** use a trusted encryption system called **AES (Advanced Encryption Standard)**.
- **MongoDB Enterprise** also uses AES, with advanced setups like AES256-CBC and AES256-GCM on Linux systems. These are high-level encryption methods that make it extremely hard for anyone without permission to read the data.

**Chat System Security:**

The chat feature in MAESTRO is also built with strong protections:

- It uses **Node.js and Socket.io** to let users chat in real time.
- All communication happens over **secure HTTPS and WSS (WebSocket Secure)** connections, so messages can't be intercepted.
- User information is stored in **MariaDB**, and passwords are securely scrambled using methods like **bcrypt**, making it almost impossible to steal them.
- Messages are saved in **MongoDB**, with strict controls that make sure only the right people can access their conversations.
- The system includes **rate limiting** and **monitoring tools** to prevent hackers from overloading the system or trying to break in using brute force.
  Finally, the platform is regularly **updated and tested for security flaws**, keeping it safe against the latest threats.

© CYberSynchorny, 2024

Table 19: List of UC3 security mechanisms.

| Name | Description |
|---|---|
| Private Cloud Deployment | MAESTRO operates solely on a private cloud infrastructure, completely isolated from the open internet, which significantly reduces the risk of external cyber threats. |
| Various Encryption mechanisms | All communications between users and the MAESTRO web application are protected using Transport Layer Security (TLS), ensuring data in transit is secure from interception or tampering.<br>Sensitive data stored in MySQL and MariaDB databases is encrypted using the Advanced Encryption Standard (AES), a robust and widely trusted symmetric encryption method.<br>MongoDB Enterprise uses AES256-CBC and optionally AES256-GCM on Linux for securing data, offering high-level protection against unauthorized access. |
| Real-Time Chat Built with Node.js and Socket.io | The chat system is powered by Node.js and Socket.io, supporting real-time messaging with security built in from the ground up. |
| Secure Communication with HTTPS/WSS | All chat data is transmitted over secure HTTPS and WebSocket Secure (WSS) connections to prevent message interception. |
| Hashed Password Storage | User passwords are stored in MariaDB using secure hashing algorithms like bcrypt, ensuring they cannot be easily stolen or reversed. |
| Access Control in MongoDB Messages | Chat messages are stored in MongoDB with strict access controls, allowing only authenticated users to read their own conversations. |
| Rate Limiting and Monitoring | Security measures such as rate limiting and continuous monitoring help protect the system from brute force and denial-of-service (DDoS) attacks. |
| Regular Security Updates and Testing | The MAESTRO platform is routinely updated and undergoes vulnerability assessments to ensure resilience against emerging threats. |

## 6.4 CYberSecurity Awareness Program

The status of current cybersecurity awareness in UC2 is described in Table 20.

Table 20: UC2 status of cybersecurity awareness

| Question | Answer |
|---|---|
| Does any cybersecurity program exist? | No |
| What is the target audience? (e.g., Generic employees, C-level, Cybersecurity/IT professionals) | First responders, Municipality police Employees |

© CYberSynchorny, 2024

| | |
|---|---|
| What tools are utilised for awareness training? | Emails and procedure documents |
| How many proficiency levels exist? | One |
| Do different cybersecurity awareness programs exist based on the target audience? | No |

## 6.5 UC2 KPIs and Objectives

The KPIs for UC2, along with their target values and mapping to CYberSynchrony modules, are presented in Table 21. These KPIs serve as the benchmark for testing the platform. The objectives of UC2 and their mapping to the KPIs are detailed in Table 22.

Table 21: UC2 KPIs and target values

| KPI # | KPI | Target | Modules for testing |
|---|---|---|---|
| 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 |

Table 22: UC2 Objectives and mapping to KPIs

| # | Objective | Related KPIs |
|---|---|---|
| UC2.O1 | Safeguard the integrity and security of online services offered to the public. | UC2.KPI1 , UC2.KPI2 |
| UC2.O2 | Implement digital IDs for secure and efficient citizen identification. | UC2.KPI4 |

© CYberSynchorny, 2024

| | | |
|---|---|---|
| UC2.O3 | Use blockchain technology for tamper-proof public records. | UC2.KPI1 |
| UC2.O4 | Develop and implement a comprehensive incident response plan for cybersecurity threats. | UC2.KPI2 |
| UC2.O5 | Train public administration staff in cybersecurity best practices and awareness. | UC2.KPI3 |

## 6.6 Scenario Definition

The scenarios that will be conducted in UC2 to evaluate the functionality and effectiveness of the CYberSynchrony platform relative to the defined KPIs are shown below.

Table 23: UC2 Test Scenario 1

| Scenario name | UC2.KPI1 |
|---|---|
| **Description** | This scenario simulates a potential unauthorized access attempt to the MAESTRO platform, which serves as critical infrastructure for the municipality of Egaleo. The goal is to test the effectiveness of integrated CYberSynchrony tools (especially CYRESCUE and CYBRITE) in detecting the threat early and preventing it from escalating. By identifying and mitigating this security event proactively, the system aims to reduce the total number of incidents that would otherwise go undetected or cause damage. |
| **Assumptions & Pre-Conditions** | • The MAESTRO platform is already operational in a private cloud environment.<br>• CYberSynchrony modules CYRESCUE and CYBRITE are fully deployed and integrated with MAESTRO's infrastructure.<br>• Historical incident data is available for baseline comparison (e.g., number of cybersecurity incidents over the past 12 months).<br>• The cybersecurity team is trained and familiar with the response workflows enabled by CYberSynchrony tools.<br>• Role-based access control and system monitoring tools are active. |
| **Goal (Successful End Condition)** | The system successfully detects and prevents a simulated unauthorised login attempt (or vulnerability exploit) before any damage occurs. Logs are recorded, notifications are sent, and no system downtime or data leakage is reported.<br>This contributes to reducing the number of successful cybersecurity incidents, helping achieve the 20% reduction KPI. |
| **Involved Actors** | • **Cybersecurity Analyst** that will monitor alerts and reacts to incidents via Cybrite dashboard |

© CYberSynchorny, 2024

| | |
|---|---|
| | • **IT administrator** to support system logging and assist with backend evaluation<br>• **Ethical Hacker** that will launch a controlled simulated attack as part of the testing |
| **Scenario Initiation** | An ethical hacker, acting as a simulated attacker, initiates an abnormal login sequence by brute-forcing admin credentials on the MAESTRO frontend. This triggers the anomaly detection systems configured in CYRESCUE. |
| **Main Flow** | 1. **Attack Simulation Begins:** Multiple failed login attempts are launched targeting a known MAESTRO admin endpoint.<br>2. **Anomaly Detected:** CYRESCUE flags the behaviour as abnormal and sends an alert to CYBRITE.<br>3. **Real-Time Alert Sent:** CYBRITE logs the event and notifies the cybersecurity analyst.<br>4. **Action Taken:** The analyst blocks the IP via the system's firewall interface and escalates for further log review.<br>5. **Post-Incident Review:** Logs from Redis, MariaDB, and MongoDB are checked to confirm no data breach occurred. The incident is recorded as "prevented" and catalogued in the incident management system. |
| **Evaluation Criteria – Related KPIs** | Compare the number of successful incidents before and after CYberSynchrony integration using MAESTRO's security logs. |
| **Modules to be validated** | CYRESCUE, CYBRITE |

Table 24: UC2 Test Scenario 2

| Scenario name | UC2.KPI2 |
|---|---|
| **Description** | This scenario tests how quickly the cybersecurity team can detect and respond to a potential credential compromise attempt targeting the MAESTRO platform. With CYberSynchrony's incident response tool (CYBRITE) fully integrated, the simulation aims to improve the platform's Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) metrics. The focus is on reducing the incident response time by at least 20% compared to baseline metrics collected before CYberSynchrony integration. |
| **Assumptions & Pre-Conditions** | • CYBRITE is fully integrated with the MAESTRO backend, log streams, and notification systems.<br>• Baseline data for response time (before CYberSynchrony deployment) is available for comparison.<br>• Egaleo's analysts have been trained to use CYBRITE workflows and follow predefined incident handling procedures.<br>• Alert thresholds and rule sets have been properly configured in CYRESCUE to detect unauthorised access attempts.<br>• Real-time alerting channels (e.g., email, SMS, dashboard pop-ups) are functioning correctly. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Goal (Successful End Condition)** | The simulated credential compromise is detected and mitigated within a time frame that is at least **20% shorter** than the average historical response time. This proves the effectiveness of the new integrated tools and improved workflows, directly supporting UC2.KP2. |
| **Involved Actors** | • **Incident Responder** that will receive alert, initiates mitigation, and closes the incident<br>• **System administrator** to verify logs, assist with account lock and forensics<br>• **Ethical Hacker** that will launch a controlled attack simulating stolen admin credentials |
| **Scenario Initiation** | An ethical hacker initiates a simulated attack using compromised admin credentials obtained through phishing. Login is attempted from a suspicious IP outside the usual geo-location and time window. This triggers the response mechanism. |
| **Main Flow** | 1. **Unusual Login Detected:** CYRESCUE flags the login based on geo-behavioural anomaly and device mismatch.<br>2. **Alert Sent Immediately:** CYBRITE receives and prioritises the event as "High Risk – Possible Account Compromise."<br>3. **Analyst Notification & Verification:** Analyst is notified via SMS and dashboard alert within 30 seconds. Logs confirm unauthorised access patterns.<br>4. **Response Initiated:** Account is locked. All active sessions under the account are terminated.<br>5. **Root Cause Investigated:** System admin checks for phishing traces or data exfiltration attempts. No damage is found; logs are archived for learning and training.<br>6. **Scenario Closed:** Event is marked as "Handled." Time to respond is logged and benchmarked. |
| **Evaluation Criteria – Related KPIs** | Compare the incident response time (from detection to containment) before and after CYberSynchrony deployment using timestamps from CYBRITE. |
| **Modules to be validated** | CYBRITE |

Table 25: UC2 Test Scenario 3

| Scenario name | UC2.KPI3 |
|---|---|
| **Description** | This scenario is designed to measure how effectively public administration staff adhere to new cybersecurity policies introduced through CYberSynchrony's CYBERWISE training module. The scenario focuses on evaluating behavioural compliance—such as correct password practices, recognition of phishing emails, secure file handling, and reporting incidents. The scenario involves simulated exercises, real-time monitoring, and post-training evaluation to determine if the targeted 95% compliance rate is achieved. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Assumptions & Pre-Conditions** | • CYBERWISE training content has been fully deployed to all relevant staff members via an LMS or internal platform.<br>• Cybersecurity policies and protocols (e.g., password renewal frequency, data handling rules) are clearly documented and accessible.<br>• Baseline compliance rate is known (e.g., previous audits showed ~70% compliance).<br>• Staff have been notified of scheduled awareness simulations (e.g., phishing tests, security quizzes).<br>• Monitoring tools are in place to track real-time behavioural compliance (e.g., password policy checks, use of secure file transfer protocols). |
| **Goal (Successful End Condition)** | At least **95% of staff** demonstrate full compliance with cybersecurity protocols during testing and post-training evaluations. This includes correctly identifying phishing attempts, updating passwords in time, securing sensitive files, and adhering to reporting guidelines. |
| **Involved Actors** | • **Municipal Police staff** that will receive cybersecurity training and participate in compliance monitoring<br>• **Cybersecurity trainer** to administer CYBERWISE training and evaluate staff behaviour<br>• **Compliance officer** that will monitor staff systems for compliance (e.g., password rules, file access)<br>• **Ethical Hacker** to send simulated phishing email<br>• **Cybersecurity analyst** to monitor response patterns |
| **Scenario Initiation** | A full compliance simulation is launched in Municipal Police department. Staff members are required to complete cybersecurity training, and are unknowingly subjected to phishing simulations and compliance tests (e.g., file transfer policy, password strength evaluation). |
| **Main Flow** | 1. **Training Delivered via CYBERWISE:** Staff complete modules on password security, phishing recognition, and data handling.<br>2. **Simulation Begins:** Team launches a simulated phishing campaign. Staff also receive prompts to update passwords and handle files per new protocol.<br>3. **Behaviour is Tracked:** The system monitors how many staff click the phishing link, fail to change passwords on time, or violate file transfer rules.<br>4. **Incident Reporting Test:** One staff member (planted actor) reports a fake security breach. Monitoring tools track how many staff escalate or ignore it.<br>5. **Post-Scenario Evaluation:** Results are collected, and compliance levels are assessed. Staff who failed are re-enrolled in targeted follow-up training.<br>6. **Compliance Report Generated:** % of total compliance is logged and compared to the 95% KPI target. |
| **Evaluation Criteria – Related KPIs** | Aggregate data from CYBERWISE completion records, phishing test results, and policy adherence logs. |
| **Modules to be validated** | CYBERWISE |

© CYberSynchorny, 2024

Table 26: UC2 Test Scenario 4

| Scenario name | UC2.KPI4 |
|---|---|
| **Description** | This scenario focuses on testing and promoting the use of digital IDs through a new **municipal mobile/web application** that allows citizens to log in securely and track incidents they have reported to the municipal police. The use case assesses how intuitive and trusted the system is, aiming to achieve a **30% increase** in digital ID adoption over a set period. |
| **Assumptions & Pre-Conditions** | • A digital ID infrastructure has been deployed and is compatible with gov.gr authentication system.<br>• The mobile/web application has been integrated with the digital ID system.<br>• Citizens are aware of the app's purpose and that it offers secure access to personal incident reports.<br>• The app is GDPR-compliant and has passed initial cybersecurity testing. |
| **Goal (Successful End Condition)** | A **30% increase** in the number of citizens using digital IDs for accessing the municipal police incident report service through the application, measured within a set time frame (e.g., 6 months from launch). Citizens must successfully log in, access their data, and engage with the app at least once. |
| **Involved Actors** | • **Citizens** that will use digital IDs to access and view municipal police reports securely<br>• **Municipal Police Dpt** to provide data on reported incidents and receive user feedback<br>• **Cybersecurity Experts** that will monitor access control, perform penetration tests, and ensure secure login and data handling<br>• **Communication team** to Lead awareness campaigns to drive digital ID adoption among citizens |
| **Scenario Initiation** | The Municipality of Egaleo launches a new app that allows residents to log in using their digital ID and view the status of any incident they have reported to the municipal police. The launch is accompanied by an awareness campaign encouraging citizens to register and use their digital ID. |
| **Main Flow** | 1. **Citizen Downloads & Launches App:** Promoted through the municipality's channels and during in-person services.<br>2. **Digital ID Login Prompt:** Citizen is asked to log in using a verified digital ID (e.g., gov.gr credentials).<br>3. **Secure Authentication Completed:** Upon success, citizen accesses a dashboard showing their submitted incidents, status updates, or assigned case officers.<br>4. **Optional Services Offered:** Citizen can report new incidents, update contact info, or leave feedback—all tied to their secure ID.<br>5. **Backend Logging:** Each secure login and session is recorded for analytics and KPI tracking.<br>6. **Feedback & Improvement:** Citizens receive surveys after interaction to gather satisfaction and usability data. Data informs future updates. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Evaluation Criteria – Related KPIs** | Set a minimum number of app user that can be considered as a successful implementation. Use login logs and authentication stats. |
| **Modules to be validated** | CYBERRA, CROSS-CORE |

© CYberSynchorny, 2024

# 7 UC3: Fortifying Universities with CYberSynchrony

## 7.1 Use Case information

The "Fortifying Universities with CYberSynchrony" use case (UC3) focuses on enhancing the cybersecurity posture of academic institutions. Universities, as open and dynamic environments, present unique cybersecurity challenges due to their diverse user base, the need for seamless access to digital resources, and the vast amounts of sensitive information they manage. This use case will integrate, test, and evaluate CYberSynchrony's security modules within the university ecosystem, identifying and mitigating vulnerabilities, responding to cybersecurity incidents and demonstrating how their advanced cybersecurity mechanisms can be effectively deployed to protect the asset of an academic setting. [16]

### 7.1.1 Use Case Needs & Motivation

The increasing reliance on digital infrastructure for education, research, and administration has made universities prime targets for cyberattacks. Threats such as phishing campaigns, ransomware incidents, and unauthorised access attempts can severely impact operations, disrupt learning processes, and compromise sensitive data. Given the interconnected nature of academic networks, the risk extends beyond individual institutions, potentially affecting collaborative research initiatives and industry partnerships.

Within this context, the UC3 leader, University of Piraeus Research Centre (UPRC), will focus on deploying and validating the CYberSynchrony framework in real-world academic scenarios. This will involve assessing vulnerabilities in university networks, testing automated threat detection and response mechanisms, and enhancing cyber resilience through coordinated defence strategies. By leveraging CYberSynchrony's capabilities, the use case aims to mitigate security risks associated with online learning platforms, student and faculty databases, and institutional IT infrastructure.

### 7.1.2 UC3 Description

The Use Case 3 (UC3) focuses on applying CYberSynchrony's security modules within the university's simulated operational environment. The aim is not only to test their technical integration but to evaluate how well these tools support the daily needs of a complex academic setting.

Particular attention will be given to key areas such as learning platforms, student services, and the university's networking infrastructure. These systems will form the basis for scenario-driven testing, helping to assess both system-level protections and user-facing responses. The findings will highlight strengths, identify areas for improvement, and contribute to more informed deployment strategies across academic institutions.

### 7.1.3 Relevance to CYberSynchrony

This use case aligns closely with CYberSynchrony's overarching objective of strengthening cybersecurity across critical infrastructures as the ones of the High Education Institutions (HEI). By applying its advanced security modules in the university environment, we will not only enhance institutional cybersecurity but also contribute valuable insights for broader applications. The ability to detect, respond to, and recover from cyber incidents in an academic setting will serve as a benchmark for securing other public and private sector domains.

UPRC, through this use case, will play a pivotal role in demonstrating the adaptability and effectiveness of CYberSynchrony's technologies. The findings will inform future iterations of the framework, ensuring that it remains responsive to the evolving threat landscape. Moreover, this initiative will foster collaboration between academic institutions, cybersecurity experts, and industry partners, reinforcing the importance of a collective approach to cyber resilience in HEIs

### 7.1.4 Roles related to testing and evaluation within UC3

The successful execution of UC3 relies on close coordination between UPRC's research team, the university's IT department, and the CYberSynchrony module leaders. Each actor has a clear role: the research team leads

© CYberSynchorny, 2024

scenario planning and evaluation design, the IT team ensures proper deployment within the live infrastructure, and the module leaders configure and monitor the tools under real conditions.

Testing will focus on threat detection, response time, and system behaviour during simulated attacks. User interaction with the system, especially during awareness and response phases, will also be monitored, providing a complete picture of technical performance and user readiness.

The roles and responsibilities within UC3 are shown in Table 27.

Table 27: Roles and Responsibilities within UC3

| Role | Responsibility in Testing and Evaluation |
|---|---|
| UPRC Research Team | Provides the architecture and defines the use cases for testing cybersecurity scenarios, including Phishing, SQL Injection, and Distributed Denial of Service (DDoS) attacks. |
| CYBRITE Module Leader | Develops and integrates the monitoring and automated response solutions for Phishing Attacks and DDoS Attacks on Domain Name System (DNS). |
| CYBERRA Module Leader | Implements and tests SQL Injection Attack detection and prevention tools (SNYK/WEKA). |
| UPRC IT Department | Deploys CYberSynchrony security tools within the university infrastructure and ensures proper configuration. |

## 7.2 System Architecture and Assets Identification

The digital infrastructure at the University of Piraeus supports a wide range of academic and administrative services. For this use case, key systems have been identified as critical to both daily operations and cybersecurity evaluation. Table 28 below outlines the main assets included in UC3 and the types of data they process.

Table 28: UC3 assets description

| Asset Name | Description | Data processed by the asset | Criticality |
|---|---|---|---|
| EClass Learning Management System (LMS) | Asynchronous learning platform and course distribution | Student credentials, assignments, course materials | High |
| Support Apps Server (Student Preregistration) | In-house system for new student onboarding | Personal documents, registration data | High |
| Student Information System (SIS) | Manages academic records, enrolment and grading | Student records, enrolment info, grades | High |
| Network Operations Center (NOC) | DNS, DHCP, AAA and secure connectivity | Network traffic, authentication logs | High |

**Learning Management System (LMS)**

The University of Piraeus' Learning Management System (LMS) is based on the open-source Open eClass platform and serves as a fundamental tool for supporting asynchronous online learning. The system is an integral part of

© CYberSynchorny, 2024

the university's digital education strategy, supporting nine undergraduate and over 40 MSc programs while seamlessly integrating with live teaching sessions.

Access to the LMS is secured through Central Authentication Service (CAS) Single Sign-On (SSO), allowing students and instructors to authenticate using institutional credentials. The platform currently supports approximately 29,000 active students and 500 instructors. It facilitates the distribution of lecture notes, exercises, and assignments while incorporating interactive content through HTML5 (H5P) technology. Additionally, it offers API integrations with external systems to enhance functionality.

Students can submit assignments, complete timed tests, and interact with instructors, ensuring a comprehensive and engaging learning experience. As a key component of the university's digital infrastructure, the LMS plays a critical role in delivering high-quality and flexible education at scale.

**Support Applications Server**

The Support Applications Server hosts internally developed applications managed by the university's IT Department. One of its key applications is the Student Preregistration System, designed to facilitate the efficient onboarding of incoming students. The system automates account setup by sending new students a one-time password via email to access the platform. It enables students to upload the necessary identification documents for validation, after which the Registry Offices process and approve the registrations. Once validated, students receive a welcome guide containing essential university resources.

Over the past two years, this system has successfully processed approximately 2,700 student registrations, significantly improving the efficiency of the onboarding process.

**Network Operations Centre (NOC)**

The Network Operations Centre (NOC) at the University of Piraeus is responsible for maintaining seamless connectivity and ensuring secure access to academic resources. As the backbone of the university's digital infrastructure, it provides a robust and centrally managed network environment that supports both educational and administrative operations.

The NOC oversees critical services such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) to maintain network stability. It also manages web hosting services for university applications and implements Authentication, Authorisation, and Accounting (AAA) mechanisms to ensure secure access control.

By maintaining a resilient and secure network environment, the NOC supports thousands of students, faculty, and staff, ensuring uninterrupted access to vital academic and administrative services.

**High-Level Infrastructure**

The infrastructure supporting the LMS, Student Preregistration System, Student Information System (SIS) and NOC services is robust and divided into clear tiers to ensure scalability and resilience (Figure 10). Below is a breakdown of the architecture.

© CYberSynchorny, 2024

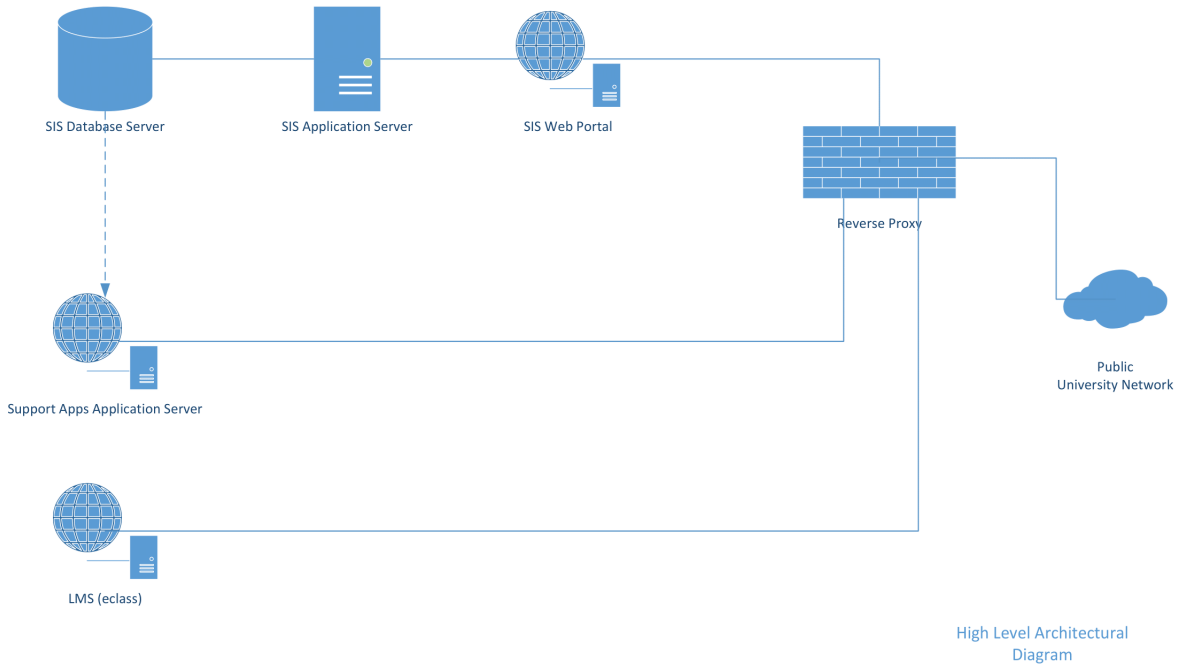


Figure 10: High-Level Architectural Diagram

**Hardware Infrastructure**

*Network Equipment:*

- **Distribution Switches:** Cisco Catalyst 3850, 3750, Huawei S6730
- **Access Switches:** Cisco Catalyst 9200, 3560, 2960, Huawei S5731
- **Central Router:** Huawei NE40
- **Core Switches:** Cisco Catalyst 9500
- **Next-Generation Firewall:** Sophos XG
- **Central Firewall:** Cisco ASA 5545 with Firepower IPS

*Server & Storage Equipment:*

Windows Server 2019 Hyper-V Failover Cluster running on a **6-node compute array** with **iSCSI SAN storage** for scalability and resilience.

© CYberSynchorny, 2024

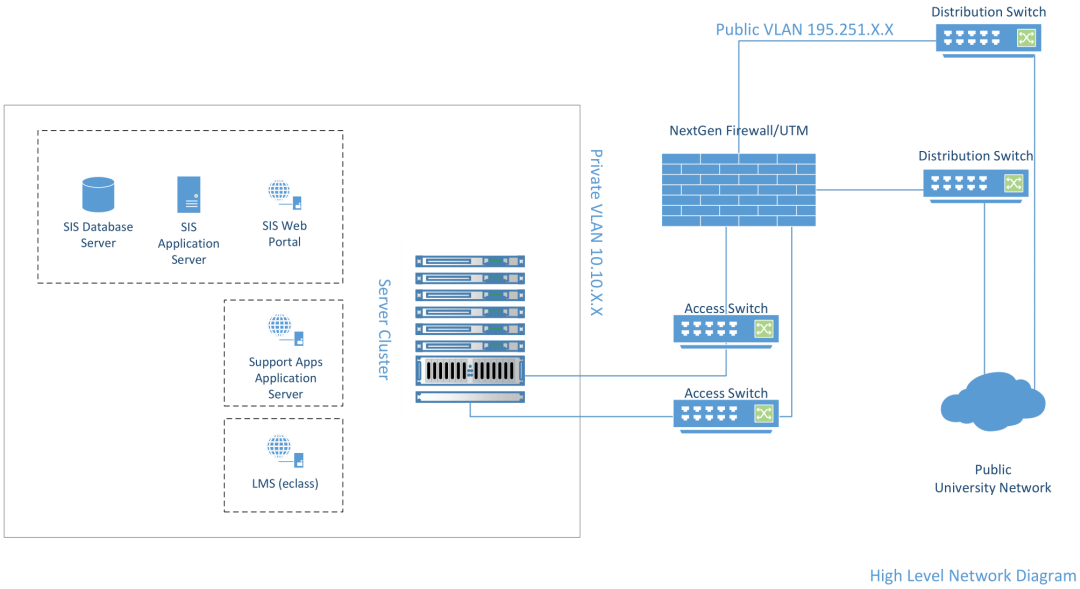


Figure 11: High-Level Network Diagram

**Software Environment**

1. **eLearning (LMS) Platform**
   **Deployment:** Monolithic Web/ Database Server (VM on Hyper-V 2019)
   **Platforms Used:**
   **O/S:** Debian Linux 10 (buster)
   **Web Server:** Apache 2. 4.38 with PHP 8.2 (HTTPS port 443)
   **Application:** GUnet Open eClass v3.15
   **Database:** MariaDB 10.3.38
   **Open source-code:**
   https://www.openeclass.org/en/download/
   https://github.com/gunet/openclass

2. **Support Apps Server**
   **Application: Student Preregistration System**
   **Deployment:** Monolithic Web/Database Server (VM on Hyper-V 2019)
   **Platforms Used:**
   **O/S:** Ubuntu 22.04.5 LTS
   **Web Server:** Apache 2. 4.38 with PHP 8.2 (HTTPS port 443)
   **Application Server:** WildFly 29.0.1.Fina
   **Application Framework**: Java 19 with Spring Boot 3.3.3
   **Database:** PostgreSQL 14.15
   **Open source-code:** Closed-source, developed in-house.

3. **Student Information System**
   **Architecture:** Three-tier system comprising a Web Portal, Application Server, and Database Server.
   **Components:**
   **Application Server:**
   **O/S**: Debian 11
   **Internal Proxy:** Apache 2. 4.38
   **Application:** Unitron v2.2.12.0 (by ILYDA S.A.)

© CYberSynchorny, 2024

**Session Cache:** Redis Server 6.0.16
**Reporting Servers:**
JasperServer 7.8.0
Apache Tomcat 8.5.57

**Database Server:**
RDBMS: SQL Server 2016 on Windows Server 2019

**Web Portal:**
**O/S:** Debian 11 Bullseye
**Internal Proxy:** Apache 2.4.38
**Application:** Unitron SIS Portal v2.1.9.0 (by ILYDA S.A.)
**Java Runtime:** Java 11 + Spring

4. **NOC Core Services**
**DNS Server:** ISC Bind 9.18 on Ubuntu 22.04.5 LTS
**DHCP Server:** ISC KEA DHCP 2.6.1 on Ubuntu 22.04.5 LTS
**Web Server:** Apache 2.4.59 with PHP 8.2 hosting WordPress 6.7.1 on Debian 12
**Radius AAA Server:** FreeRADIUS 3.2.4 on Ubuntu 22.04.5 LTS

To support the integration and evaluation of CYberSynchrony modules, it is important to understand the underlying network structure that connects and secures all institutional services. The diagram below outlines the university's core networking environment and the services involved:

© CYberSynchorny, 2024

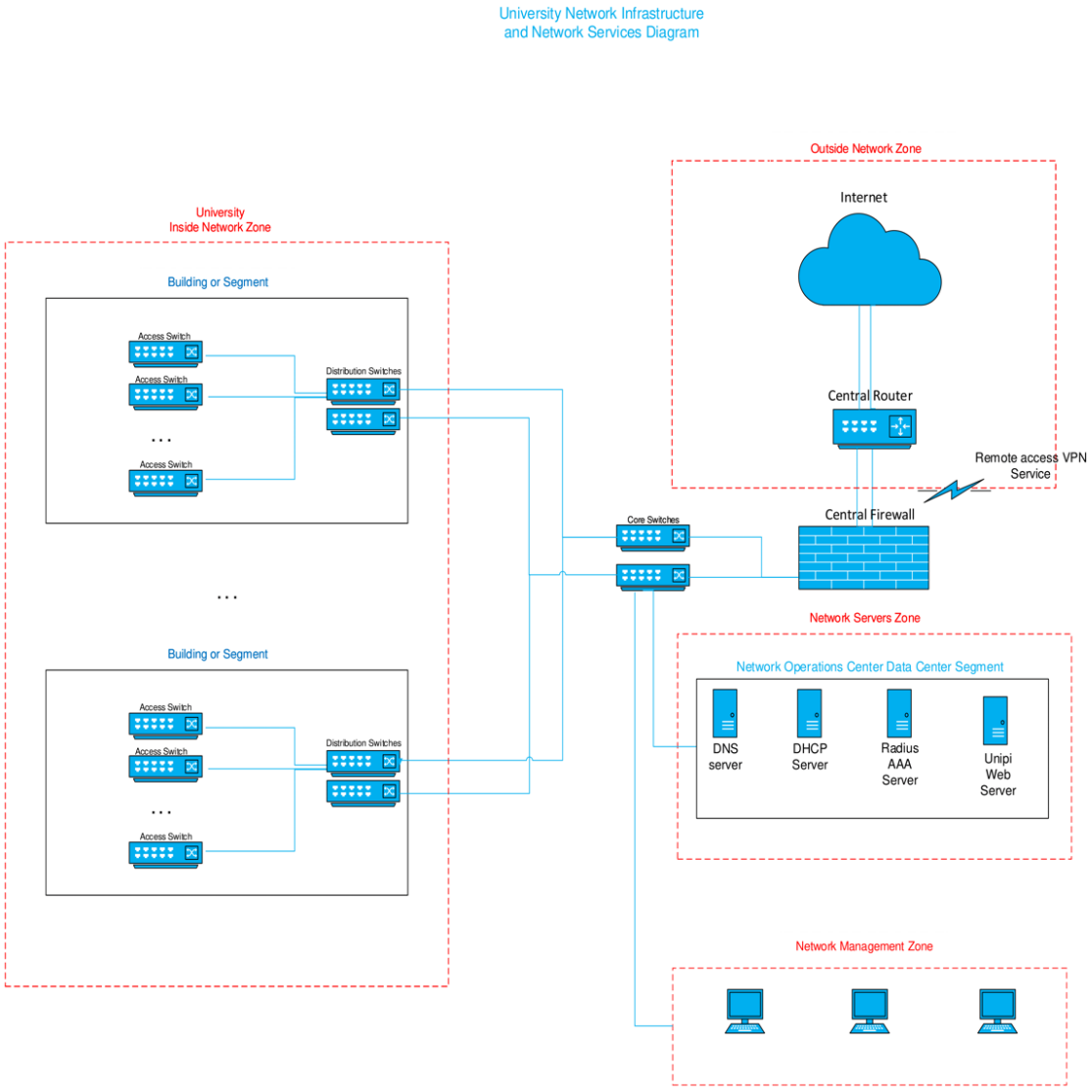


Figure 12: University Network Infrastructure and Network

**Network Infrastructure**

*Network Zones:*

- **University Network Zone**
  - Comprises multiple buildings or segments.
  - Each building contains:
    - Access Switches
    - Distribution Switch aggregating the access layer.
  - Distribution switches connect to the Core Switches.
- **Outside Network Zone**
  - Represents the external Internet.
  - Connected to the internal network via a Central Router.
  - A Remote Access Virtual Private Network (VPN) Service is shown linking the external zone to the internal network.
  - The Central Router connects to the Central Firewall.

© CYberSynchorny, 2024

- **Network Servers Zone**
  - Labeled Network Operations Center Data Center Segment.
  - Contains 4 core servers:
    - DNS Server
    - DHCP Server
    - Radius AAA Server
    - Unipi Web Server
  - Connected directly to the Core Switches.
- **Network Management Zone**
  - Displays 4 monitoring/management PCs.
  - Connected to the core switching infrastructure.

The systems and infrastructure described in this section represent the foundation on which UC3 testing activities will be carried out. By understanding the university's existing architecture and services, we can more precisely deploy CYberSynchrony components and evaluate their performance in real operational conditions. The next section focuses on the security mechanisms already in place and the awareness landscape across the university community.

## 7.3 Current Security Mechanisms

The current security mechanisms within the UC3 infrastructure are shown in Table 29.

Table 29: List of UC3 security mechanisms.

| Name | Description |
|---|---|
| User & Staff Training | Regular cybersecurity awareness sessions for staff and students, covering safe practices and breach-reporting procedures. |
| Network security | Next-Generation Firewalls (e.g., Sophos XG, Cisco ASA with Firepower IPS) and filtering rules to protect internal resources |
| Access Controls & AAA | FreeRADIUS for Authentication, Authorisation, and Accounting, plus strong password policies and Multi-Factor Authenticator (MFA) where supported |
| Endpoint Protection | Basic antivirus on PCs and laptops, OS patching, and secure configurations for servers (Debian, Ubuntu, Windows Server). |
| Vulnerability Scanning | Periodic scans (including web app checks for LMS, SIS), plus regular patch management to mitigate newly discovered threats |

The above mitigation actions secure the educational activities.

## 7.4 CYberSecurity Awareness Program

In addition to technical safeguards, the human factor plays a key role in the institution's cybersecurity posture. The University of Piraeus has made recent progress in raising cybersecurity awareness, particularly among administrative and IT staff.

© CYberSynchorny, 2024

The status of current cybersecurity awareness in UC3 is described in Table 30.

Table 30: UC3 status of cybersecurity awareness

| Question | Answer |
|---|---|
| Does any cybersecurity program exist? | Basic awareness campaigns in place |
| What is the target audience? | Administrative Staff, IT Professionals |
| What tools are utilised for awareness training? | Internal emails, security checklists |
| How many proficiency levels exist? | One |
| Do different cybersecurity awareness programs exist based on the target audience? | No |

This structured approach ensures that future training initiatives can be tracked, adapted, and evaluated based on real data. It also provides a starting point for tailoring cybersecurity content to specific university functions and improving overall resilience against social engineering and human-error-based attacks.

## 7.5 UC3 KPIs and Objectives

The objectives of UC3 focus on strengthening the cybersecurity posture of the university's digital infrastructure, ensuring faculty and student adherence to security protocols, and improving the institution's ability to respond to cyber incidents. These objectives are directly linked to a set of Key Performance Indicators (KPIs), which provide measurable thresholds to assess impact and monitor progress over time.

Each KPI is defined with a clear performance target, and its evaluation is based on a combination of quantitative monitoring tools and qualitative assessment methods. Evidence will be collected through log analysis, behaviour tracking, user feedback, and structured reporting processes.

The KPIs for UC3, along with their target values and mapping to CYberSynchrony modules, are presented in Table 31. These KPIs serve as the benchmark for testing the platform. The objectives of UC3 and their mapping to the KPIs are detailed in Table 32.

Table 31: UC3 KPIs and target values

| KPI # | KPI | Target | Modules for testing |
|---|---|---|---|
| UC3.KPI1 | Number of incidents | Number of cybersecurity incidents detected and resolved decreased by 20% post-implementation. | CYRESCUE, CYBRITE |
| UC3.KPI2 | Faculty compliance rates | Faculty compliance rates with new cybersecurity protocols achieve 90% compliance post-training and awareness campaigns. | CYBERWISE |
| UC3.KPI3 | Student cybersecurity satisfaction | Student satisfaction rates with new security of online services | CYBERGOPLUS |

© CYberSynchorny, 2024

| | | | |
|---|---|---|---|
| | | achieve 90% satisfaction post-enhancements. | |
| UC3.KPI4 | Response time | Time takes to respond to cybersecurity incident reduced by 30% post SOAR platform deployment. | CYBRITE |

Table 32: UC3 Objectives and mapping to KPIs

| # | Objective | Related KPIs |
|---|---|---|
| UC3.O1 | Guarantee the integrity and safety of e-learning platforms utilised by the institution. | UC3.KPI1 , UC3.KPI4 |
| UC3.O2 | Put in place strong digital security measures to safeguard critical research data. | UC3.KPI1 |
| UC3.O3 | Ensure the confidentiality and integrity of student academic and personal records. | UC3.KPI3 |
| UC3.O4 | Equip teaching staff with the knowledge and skills needed for cybersecurity best practices. | UC3.KPI2 |
| UC3.O5 | Formulate and execute a detailed plan for handling cybersecurity incidents. | UC3.KPI4 |

The mapping of objectives to KPIs ensures a direct connection between institutional goals and measurable outcomes. This structure provides a clear pathway for evaluating progress throughout the pilot phase and for identifying areas where additional focus or adjustments may be required.

## 7.6 Scenario Definition

To evaluate the robustness of CYberSynchrony's cybersecurity modules in an academic environment, the University of Piraeus Research Centre (UPRC) has developed a set of structured scenarios tailored to simulate and assess common cyber threat vectors affecting university infrastructures. Each scenario is mapped to specific KPIs that reflect institutional cybersecurity performance and resilience.

The three core scenarios developed by UPRC simulate realistic and high-impact incidents:

1. A phishing attack targeting university staff and students.
2. A SQL Injection attempt against the Learning Management System (LMS).
3. A Distributed Denial of Service (DDoS) attack targeting the university's DNS infrastructure.

© CYberSynchorny, 2024

These scenarios are designed to validate detection, response, mitigation, and awareness capabilities across CYberSynchrony tools such as CYBRITE, CYBERRA, and CYBERWISE. Each scenario outlines the threat context, preconditions, actors involved, execution flow, and how success is measured. This structured approach provides the foundation for piloting, validation, and eventual replication of the cybersecurity measures within academic environments across the EU.

Table 33: UC3 Test Scenario 1

| Scenario name | UC3.KPI1 Phishing Attack on Academic Community |
|---|---|
| **Description** | A crafted phishing email bypasses basic filters and targets university users. A student clicks the link, leading to credential harvesting and anomalous login. CYBRITE detects anomalies, and CYRESCUE coordinates incident response actions. |
| **Assumptions & Pre-Conditions** | Users actively access institutional emails and LMS. CYBRITE and CYRESCUE modules are deployed and integrated. No prior alerts in the past 30 days. |
| **Goal (Successful End Condition)** | Detect the attack, contain compromised accounts, and initiate incident handling workflows. |
| **Involved Actors** | UPRC Research Team, UPRC IT Department, Faculty & Students, CYBRITE Team, CYRESCUE Team |
| **Scenario Initiation** | A simulated phishing campaign is launched internally. |
| **Main Flow** | Step 1:<br>Phishing email is delivered to 100 test participants.<br><br>Step 2:<br>Some users click the link, simulating credential theft.<br><br>Step 3:<br>CYBRITE logs anomalous login events (e.g., location/time mismatch).<br><br>Step 4:<br>CYRESCUE triggers incident response procedures, including account containment and alert notification.<br><br>Step 5:<br>Affected accounts are reset and follow-up actions logged. |
| **Evaluation Criteria – Related KPIs** | UC3.KPI1 – Number of cybersecurity incidents detected and resolved decreased by 20% post-implementation |

© CYberSynchorny, 2024

| | |
|---|---|
| **Modules to be validated** | CYRESCUE, CYBRITE |

Table 34: UC3 Test Scenario 2

| **Scenario name** | **UC3.KPI2 Faculty Cybersecurity Compliance Program** |
|---|---|
| **Description** | The CYBERWISE module is used to launch and monitor a university-wide compliance initiative targeting faculty members. The objective is to improve adherence to cybersecurity protocols, including MFA usage, password policy compliance, and secure login practices. |
| **Assumptions & Pre-Conditions** | Faculty members have institutional accounts. CYBERWISE is fully integrated with the training system, login monitoring tools, and policy acknowledgements. |
| **Goal (Successful End Condition)** | Achieve at least 90% faculty compliance with cybersecurity policies as verified through system-based behavior logs. |
| **Involved Actors** | UPRC Research Team, UPRC IT Department, CYBERWISE Team, Faculty Members |
| **Scenario Initiation** | An awareness and compliance campaign is launched across all faculty departments. |
| **Main Flow** | Step 1:<br>CYBERWISE distributes required cybersecurity training, policy documents, and compliance checklists.<br><br>Step 2:<br>Faculty are required to complete training and acknowledge policy changes via digital forms.<br><br>Step 3: The system tracks MFA enablement, password changes, and policy acknowledgement.<br><br>Step 4:<br>Automated reports are generated identifying compliant and non-compliant users.<br><br>Step 5:<br>Targeted follow-up emails are sent to non-compliant individuals.<br><br>Step 6:<br>Final compliance rate is calculated. KPI is met if ≥90% of faculty are marked compliant. |

© CYberSynchorny, 2024

| | |
|---|---|
| **Evaluation Criteria – Related KPIs** | UC3.KPI2 – Faculty compliance rates with new cybersecurity protocols achieve 90% compliance post-training and awareness campaigns |
| **Modules to be validated** | CYBERWISE |

Table 35: UC3 Test Scenario 3

| **Scenario name** | **UC3.KPI3 Student Satisfaction with Cybersecurity of Digital Services** |
|---|---|
| **Description** | This scenario focuses on evaluating student satisfaction regarding the cybersecurity of the university's digital academic services. The objective is to validate the effectiveness of the CYBERGOPLUS module in enhancing user trust and perceived security. The satisfaction level is measured through structured feedback, collected after the module is operational in the university's digital environment. |
| **Assumptions & Pre-Conditions** | The CYBERGOPLUS module has been deployed and integrated into the university's core digital services. These services are regularly accessed by students for academic processes such as course registration, digital document access, and grade viewing. A preliminary satisfaction survey has already been conducted to establish baseline values. The environment has remained operationally stable during the period of student interaction with the deployed components. |
| **Goal (Successful End Condition)** | Achieve a minimum of 90% positive satisfaction rate in student feedback regarding the security and trustworthiness of digital academic services. |
| **Involved Actors** | UPRC Research Team, UPRC IT Department, Academic Services Office, CYBERGOPLUS Team, University Students |
| **Scenario Initiation** | The evaluation begins after the successful deployment of CYBERGOPLUS across university digital platforms and a sufficient period of student usage. Surveys are distributed to collect structured feedback from student users. |
| **Main Flow** | Step 1:<br>A pre-deployment survey is conducted among students to measure the baseline satisfaction level related to digital service security.<br><br>Step 2:<br>CYBERGOPLUS is deployed across relevant university platforms.<br><br>Step 3:<br>Students are notified of the improvements and continue to use the services under normal conditions. |

© CYberSynchorny, 2024

| | |
|---|---|
| | Step 4:<br>After a representative period of use, a post-deployment survey is distributed, focusing on perceived improvements in data protection, access control, and trust in system security.<br><br>Step 5:<br>Responses are collected and analysed, comparing results against baseline data.<br><br>Step 6:<br>The KPI is considered met if ≥90% of the participants express satisfaction or improved trust. |
| **Evaluation Criteria – Related KPIs** | KPI3 - Student satisfaction rates with new security of online services achieve 90% satisfaction post-enhancements. |
| **Modules to be validated** | CYBERGOPLUS |

Table 36: UC3 Test Scenario 4

| **Scenario name** | **UC3.KPI4 DDoS Attack on University DNS** |
|---|---|
| **Description** | A DDoS flood targets the ISC Bind DNS server, disrupting domain resolution across academic services. CYBRITE is used for detection, logging, and automated response to restore service and assess performance. |
| **Assumptions & Pre-Conditions** | DNS logs are collected, the system supports Anycast and rate-limiting, and CYBRITE is active across network monitoring zones. |
| **Goal (Successful End Condition)** | Detect and mitigate the attack in under 10 minutes. Ensure DNS uptime remains >99.5%. |
| **Involved Actors** | UPRC Research Team, CYBRITE Module Team, UPRC NOC |
| **Scenario Initiation** | DDoS attack simulation tool targets DNS with recursive query flood. |
| **Main Flow** | Step 1:<br>Volumetric traffic targets Bind DNS service.<br><br>Step 2:<br>CYBRITE identifies traffic surge and logs event.<br><br>Step 3:<br>Automated playbooks filter queries and redirect via Anycast. |

© CYberSynchorny, 2024

| | |
|---|---|
| | Step 4:<br>NOC confirms service recovery and logs outcomes.<br><br>Step 5:<br>Reports are generated on time-to-containment and response performance. |
| **Evaluation Criteria – Related KPIs** | UC3.KPI4 – Time taken to respond to cybersecurity incident reduced by 30% post SOAR platform deployment |
| **Modules to be validated** | CYBRITE |

These scenario definitions will support the evaluation of CYberSynchrony's capabilities under WP8 and inform the subsequent validation and training activities. They serve as structured blueprints for pilot deployments at UPRC and are subject to further refinement based on pilot results.

© CYberSynchorny, 2024

# 8 Conclusions

Deliverable *D8.1 – CYberSynchrony Integration Blueprint & Use Case Portfolio V1*, part of WP8 (Integration, Demonstration, and Evaluation), lays the foundation for the comprehensive integration of CYberSynchrony modules and their practical evaluation through targeted use cases. It is structured to systematically address the integration and validation of the CYberSynchrony ecosystem in diverse operational environments.

The **Methodology for Integrating the CYberSynchrony marketplace** provides a detailed roadmap that guides the structured development and deployment of the platform's components, ensuring resilience, scalability, and compatibility with various IT infrastructures. The integration is defined across three main architectural layers:

- Cloud Deployment Layer: Hosts core runtime services and anomaly detection components with Kubernetes for scalability.
- On-Premise Deployment Layer: Manages local agents and data preparation that securely feed information into the cloud.
- Standalone Tools Layer: Includes on-demand modules for forensic analysis and risk profiling.

The Integration Methodology also presents a comprehensive inventory of tools, systematically mapping each to its role within the platform. This ensures alignment with the architecture, anticipates interoperability challenges, and facilitates smooth integration. The Overview of Components (Tools) describes the technologies and their deployment locations, interfaces, and data flows, supporting seamless data exchange and coordinated responses. Additionally, the Communication Interfaces and Data Exchange outlines the necessary environmental and technical prerequisites for each component, supporting streamlined and predictable deployments.

The **Methodology for Testing the CYberSynchrony marketplace** focuses on validating the platform in real-world scenarios. It defines use case needs, roles, system architecture, and critical assets to ensure reliability, performance, and compatibility with existing infrastructures, thereby establishing robust cybersecurity measures. The deliverable then details three specific Use Cases' (UCs) portfolio, to demonstrate the platform's application:

- UC1: Demonstrating Comprehensive CyberHealth Security for Digital Healthcare (AMC): Focuses on protecting Electronic Health Records (EHRs), telemedicine systems, and internal communications in healthcare settings.
- UC2: CYberSynchrony-Powered Public Administration (EGL): Enhances cybersecurity for public administration through the MAESTRO platform, securing emergency response coordination and incident management.
- UC3: Fortifying Universities with CYberSynchrony (UPRC): Addresses cybersecurity in academic environments, focusing on protecting LMS platforms, student records, and critical university infrastructure.

Across these three UCs, the deliverable demonstrates the platform's effective integration and validation in critical environments, highlighting how CYberSynchrony addresses sector-specific cybersecurity threats. The insights gained from this validation will guide further enhancements and wider adoption of the platform across various infrastructures, supporting the project's broader goal of establishing a secure, modular cybersecurity framework for critical sectors.

The final version of the deliverable, D8.4, due on month 36, will present the final integration roadmap, further elaborate on the work carried out to integrate the CYberSynchrony tools into the platform, and provide comprehensive reporting on the validation activities conducted across the three use cases. This final iteration will consolidate the findings and improvements identified during the initial integration phase, ensuring that the platform is robust, scalable, and fully aligned with the cybersecurity requirements of the targeted sectors.

© CYberSynchorny, 2024

# 9 References


[1] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., ... & Warfield, A. (2003). *Xen and the art of virtualization*. ACM SIGOPS Operating Systems Review, 37(5), 164-177.

[2] Docker (2025). *Docker Overview*. Available at: https://docs.docker.com/get-started/overview/

[3] Kubernetes (2025). *Kubernetes Concepts*. Available at: https://kubernetes.io/docs/concepts/

[4] Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2019). *Kubernetes: Up & Running: Dive into the Future of Infrastructure*. O'Reilly Media, Inc.

[5] Hightower, K., Burns, B., & Beda, J. (2017). *Kubernetes: The Complete Guide to Managing Containers at Scale*. O'Reilly Media, Inc.

[6] Kim, G., Humble, J., Debois, P., & Willis, J. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations*. IT Revolution.

[7] Istio (2025). *Istio Architecture and Security*. Available at: https://istio.io/latest/docs/

[8] Fielding, R. T. (2000). *Architectural Styles and the Design of Network-based Software Architectures* (Doctoral dissertation, University of California, Irvine).

[9] *GraphQL Documentation*. Available at: https://graphql.org/learn/

[10] gRPC (2025). *gRPC Concepts and Architecture*. Available at: https://grpc.io/docs/

[11] Fette, I., & Melnikov, A. (2011). *The WebSocket Protocol*. IETF RFC 6455.

[12] National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[13] OWASP (2024). *OWASP Testing Guide v5.0*. Available at: https://owasp.org/www-project-web-security-testing-guide/

[14] 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.

[15] Mora, L., Bolici, R., & Deakin, M. (2017). *The first two decades of smart-city research: A bibliometric analysis*. Journal of Urban Technology, 24(1), 3-27.

[16] Davis III, C. S., Oliveira, D. S., & Wendi, G. (2020). *Cybersecurity for Higher Education Institutions: Awareness and Training*. IEEE Access, 8, 144126-144136.


© CYberSynchorny, 2024

# Annex I: Tools communication matrix

| Partner | Component | MISP | | Wazuh | | Suricata | | WEKA | | SNYK | | Human RM (HRM) | | Anomaly Detector IDS | | Data Integrity & Encryption (Dist HyperLedger) | | Kitsune Monitoring | | Kitsune Search | | CyberSecurityPostureAssessment (CSPA) | | AttackSurfaceAssessment( ASA) | | Purple TeamAssessment (PTA) | | SecurityBreachSimulation (SBS) | | Defensive Cyber Operations (DCO) (Response Playbooks) | | Sysmon | | Data Preparation Module | | Social Engineering | | Policy Tools | | CYberSynchrony Platform | | Cloud Storage | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface | Data Flow Direction | Interface |
| IANUS | MISP | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| IANUS | Wazuh | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↗ (Send) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| IANUS | Suricata | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| TRUST | WEKA | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| TRUST | SNYK | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| TRUST | Human RM (HRM) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| MAG | Anomaly Detector IDS | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| BYTE | Data Integrity & Encryption (Dist HyperLedger) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↕ (Exchange) | HTTPS | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| MER | Kitsune Monitoring | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| MER | Kitsune Search | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| FP | CyberSecurityPostureAssessment (CSPA) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | ↙ (Receive) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| FP | AttackSurfaceAssessment( ASA) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↗ (Send) | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| FP | Purple TeamAssessment (PTA) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| FP | SecurityBreachSimulation (SBS) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| FP | Defensive Cyber Operations (DCO) (Response Playbooks) | Not Applicable | Not Applicable | ↙ (Receive) | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| IANUS | Sysmon | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| BYTE | Data Preparation Module | Not Applicable | Not Applicable | ↙ (Receive) | HTTPS | ↙ (Receive) | HTTP | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↕ (Exchange) | HTTPS | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↙ (Receive) | HTTPS | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| - | Social Engineering | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| - | Policy Tools | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| MAG | CYberSynchrony Platform | Not Applicable | Not Applicable | ↙ (Receive) | REST | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↕ (Exchange) | REST | ↕ (Exchange) | REST | Not Applicable | Not Applicable | ↕ (Exchange) | REST | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | | Not Applicable | Not Applicable |
| - | Cloud Storage | ↕ (Exchange) | HTTPS | ↕ (Exchange) | HTTPS | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | ↙ (Receive) | HTTPS | Not Applicable | Not Applicable | ↗ (Send) | HTTPS | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | | |

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. 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.