Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D6.3 Pilots final phase report

Version: V2.2

Work package	WP 6
Task	Task 6.3
Due date	30/11/2025
Submission date	30/11/2025
Deliverable lead	OPBG
Version	2.2
Authors	Alberto E. Tozzi (OPBG), Campia Ginevra (OPBG), Diana Ferro (OPBG)
Reviewers	Andrés Castillo (FHUNJ), Santiago Bollain (FHUNJ)

Abstract	This derivable describes the main activities performed during the last phase of Pilot 1 and Pilot 2. This document provides a detailed analysis of the implementation and validation of each tool within every pilot and the challenges encountered during the process.
Keywords	Pilots, tools, implementation, integration and validation

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V 1.0	12/06/2025	Original draft	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG)
V 1.1	01/10/2025	Contributions of partners defined	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG), Diana Ferro (OPBG), Andrea Scaburri (MCI), Simone Favrin (MCI), Esteban Armas (EVIDEN), Juan Carlos Perez Baun (EVIDEN), Hrvoje Ratkajec (XLAB), Andrès Castillo (FHUNJ), Santiago Bollain (FHUNJ), Hrvoje Ratkajec (RGB), João Rodrigues (INOV)
V 1.2	10/11/2025	Collection of all partners contributions	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG), Diana Ferro (OPBG), Andrea Scaburri (MCI), Simone Favrin (MCI), Esteban Armas (EVIDEN), Juan Carlos Perez Baun (EVIDEN), Hrvoje Ratkajec (XLAB), Andrès Castillo (FHUNJ), Santiago Bollain (FHUNJ), Hrvoje Ratkajec (RGB), João Rodrigues (INOV)
V 2.0	14/11/2025	First completed version for internal review	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG), Simone Favrin (MCI)
V 2.1	25/11/2025	First internal review	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG)
V 2.2	26/11/2025	Final version after internal review	Alberto E. Tozzi (OPBG), Ginevra Campia (OPBG), Andrea Scaburri (MCI), Simone Favrin (MCI)

Disclaimer

Copyright notice

Funded by Horizon Europe Framework Programme of the European Union

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**X**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

The CYLCOMED project developed a cybersecurity framework for connected medical devices (CMDs) via a cybersecurity toolbox. The aim of the project is to enhance cybersecurity in clinical ecosystems by ensuring confidentiality, integrity, and availability of patient data. To demonstrate and validate the CYLCOMED toolbox in real-life settings, its testing has been performed in two pragmatic pilots, following guidelines and standards for the integration with the emerging technologies:

Pilot 1 - simulated hospital equipment cybersecurity in an Intensive Care Unit (ICU) setting using digital twins (no human data) for specific legacy devices, represented by infusion pumps, that have been enhanced with a new controller module with the aim of strengthening cybersecurity to protect patients' data and system integrity. The pilot evaluated system performance and security risk upon the integration of safeguards against threats like unauthorized access and data breaches.

Pilot 2 - focused on telemedicine platforms, validated through real-world scenarios conducted in hospital settings (deployment A) and in a virtual, simulated environment (deployment B). The first one used certified medical device in the hospital's framework, investigating different aspects (cardiac paediatric patients, clinical workflow) and included tools integration, supporting real-time monitoring and ethical compliance, while fostering collaboration between clinicians and technical teams. The second deployment consists of a VM where the telemonitoring platform was installed and integrated with all the tools developed in CYLCOMED. Furthermore, being deployment B a safe environment, it was used to perform some simulated attacks to evaluate the tools performances. This controlled environment supported thorough testing, ensured safety and flexibility for experimentation.

The final-phase and validation report of the CYLCOMED project presents the culmination of a multi-phase effort to develop, integrate, and evaluate a cybersecurity toolbox designed for connected medical devices and digital health infrastructures. Overall, the CYLCOMED project successfully delivered a validated, clinically aligned cybersecurity solution, ready for further development in both hospital and telehealth settings. The complementary nature of the two pilots ensures a holistic assessment of the toolbox, confirming its technical robustness, clinical applicability, and scalability across different healthcare scenarios.

The final phase validation presents the results of the CYLCOMED cybersecurity toolbox deployed in hospitals and telemonitoring settings. Combining technical stress tests, interoperability trials, and stakeholder interviews conducted at Pilot sites, the validation confirms the platform’s initial clinical fit and technical robustness.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

List of tables

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

AI	Artificial Intelligence
ARDS	Acute respiratory distress syndrome
CP-ABE	Cyphertext-Policy Attribute-Based Encryption
CET	Territorial Ethical Committee
CHD	Congenital Heart Disease
CMD	Connected Medical Device
CTI	Cyber Threat Intelligence
CTQT	Clinical Trial Quality Team
CUB	Charité – Universitätsmedizin Berlin
CUDA	Compute Unified Device Architecture
CV	Cardiovascular
CYLCOMED	CYbersecurity tooLbox for COnnected MEdical Devices
DPO	Data Protection Office
ECG	Electrocardiogram
eCRF	Electronic Case Report Form
EHR	Electronic Health Records
ENS	Spain Esquema Nacional de Seguridad
EU	European Union
EVIDEN	Formerly Atos
FE4MED	Functional Encryption for Medical Data
FHUNJ	Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús
FN	False Negative
FP	False Positive
GCP	Good Clinical Practice

Funded by Horizon Europe Framework Programme of the European Union

GDPR	General Data Protection Regulation
HF	Heart Failure
HIS	Hospital Information System
ICU	Intensive Care Unit
INOV	Inov - Instituto De Engenharia De Sistemas E Computadores, Inovação
IoMT	Internet of Medical Things
IT	Information technology
IVDR	In Vitro Diagnostic Medical Devices
KUL	Katholieke Universiteit Leuven
LADS	Live Anomaly Detection System
LOMOS	LOg MOnitoring System
LOPDGDD	Organic Law on Protection of Personal Data and Guarantee
LuS4MED	Ledger uSelf for Medical Data
MCI	MediaClinics Italia
MDR	Medical Devices Regulation
MHP	Mediaclinics Health Platform
NMT	NeuroMuscular Transmission
OPA	Open Policy Agent
OPBG	Ospedale Pediatrico Bambino Gesù
OTA	Over The Air
RGB	RGB Medical Devices
RMSE	Root Mean Sqare Error
ROI	Return of Investement
RPI	Rasberry PI
SaMD	Software as Medical Device

Funded by Horizon Europe Framework Programme of the European Union

SIEM	Security Information and Event Management
SIV	Site Initiation Visit
SOC	Security Operation Center
SSI	Synchronous Serial Interface
SSO	Single Sign-On
SUS	System Usability Scale
TCO	Total Cost of Ownership
TN	True Negative
TP	True Positive
VC	Verifiable Credential
WP	Work Package
XLAB	XLAB Razvoj Programske Opreme in Svetovanje

Funded by Horizon Europe Framework Programme of the European Union

Structure of the document

This report is structured as follows:

- Section 1: describes the objectives of the Report
- Section 2: presents a brief description of the cybersecurity tools and risk assessment tool developed within the project, followed by the explanation of their development, implementation and integration into the two pilots, included any challenges faced during these phases
- Section 3: explains the validation process of the CYLCOMED system into the real-world and simulated scenarios

Funded by Horizon Europe Framework Programme of the European Union

1 Objectives of the Report

The objective of **Deliverable 6.3**, titled 'Pilots Final Phase Report', is to provide a comprehensive overview of the project's progress and outcomes, focusing on the final round of implementation and the complete validation process of the CYLCOMED toolboxes within the two Pilots: As a key output of Work Package 6, this report not only documents the technical deployment and end-user feedback but also demonstrates the practical implementation of the solutions developed throughout the project:

This final phase of the toolbox validation is tightly connected to CYLCOMED's overreaching ambition: ***to strengthen the cybersecurity of Connected Medical Devices (CMDs) in an increasingly complex digital health landscape.*** The pilots served as a critical testbed to evaluate the integration of end-user-driven cybersecurity tools and methodologies, ensuring they respond effectively to clinical needs, infrastructure constraints, and real-time operational challenges.

1.1 Purpose and coverage of the Report

This report refers to the last phase of the project, from M24 to M36, with the aim to provide an update regarding the final phase of the cybersecurity toolbox implementation and validation in the Pilot 1 and 2.

More specifically the report covers the following aspects:

- **Final Implementation:** it explains the last steps of the CYLCOMED toolboxes implementation into real-world scenarios through the project's pilots.
- **Validation Results**: It presents the results of the validation of the CYLCOMED toolbox in simulations and **real-world scenarios**. The project aims to demonstrate the effectiveness and user-friendliness of its toolbox by integrating it into dedicated pilots and validating the solutions in relevant environments.
- **Multidisciplinary Validation**: The validation conducted in WP6, and thus reported in D6.3, is not limited to mere technical aspects. While it assesses the ease of integration and performance, it also comprehensively covers **non-technical dimensions**. These non-technical aspects include: Usability, Value perceived by the user, Societal aspects, Legal and Ethical aspects, Exploitability for future use or commercialization.

1.2 The Pilots

This section presents a brief recap of the two pilots, with the aim to demonstrate the CYLCOMED's toolbox relevance into the hospital equipment and telemonitoring scenarios.

1.2.1 Pilot 1: Hospital Equipment

Pilot 1 refers to patients suffering from acute respiratory distress syndrome (ARDS) in hospital Intensive Care Units (ICUs), who rely on mechanical ventilation as a life-saving measure. An improved outcome of the most severely ARDS affected patients has been seen with Neuromuscular blocking agents (NMBAs), by improving ventilatory support, reducing mortality and facilitating recovery. However, the automated dosage delivery and neuromuscular transmission (NMT) control must be carefully monitored and protected against potential cybersecurity threats.

Funded by Horizon Europe Framework Programme of the European Union

In this context, CYLCOMED integrates a new NMT monitoring technique (NMTCuff) and automated infusion control into RGB Medical's Vision Air monitor. This Pilot has been carried out al laboratory level using a digital twin and Hardware/Software-in-Loop setup which tests cybersecurity features like user authentication, AI-based anomaly detection, and device integrity checks to ensure resilience and secure operation. This solution aims to prevent cybersecurity threats and provides a scalable framework for connected critical care devices.

1.2.2 Pilot 2: Telemonitoring

In Pilot 2 a special attention has been given to telemedicine platforms used to remotely monitor patients with specific medical conditions.

The Pilot is split into two deployments: one in real-world hospital settings and another in a controlled, virtual environment.

Deployment A is conducted in hospitals with paediatric cardiac patients, integrating CYLCOMED tools into existing clinical workflows to ensure real-time cybersecurity monitoring while maintaining patient safety and privacy.

Deployment B occurs in a virtual and in a controlled environment, allowing for in-depth testing of the CYLCOMED toolbox, providing the perfect environment to test most of CYLCOMED tools overcoming technical and ethical limitations. Specifically, the VM environment in MCI servers has been used to test the AI-based threat detection and simulated cyber-attacks, without involving real patients or systems. This deployment focused also on transit ambulance situations and AI model evaluation investigating the potential for improving threat analysis, a crucial component of the analysis and monitoring tools. In this situation, the capacity to identify network irregularities becomes essential for safeguarding patient information. These sub-pilots have also been used in a controlled setting due to organisational and ethical requirements.

Funded by Horizon Europe Framework Programme of the European Union

2 Activities completed in each Pilot Study

During the last phase of the project, the consortium focused on the pilot's execution. Meanwhile, the technical partners, having completed development of the tools during the first piloting cycle (M7-M24) (D6.2), concentrated on their implementation and integration in the different scenarios covered by the pilots.

2.1 CYLCOMED Toolbox: software tools

LOg MOnitoring System (LOMOS)

LOMOS is an advanced log monitoring system that uses Natural Language Processing (NLP) techniques to automatically detect anomalies in system and application logs, indicating potential security threats. Unlike traditional rule-based methods, LOMOS builds behavioural models through deep learning approaches like Masked Language Modelling and Hypersphere Volume Minimization to analyse log patterns without manual intervention. This enables real-time, intelligent monitoring of system behaviour, providing insights into both current and past asset status.

Live Anomaly Detection System (LADS)

As described in deliverables D5.1, D5.2, and D5.3, LADS is an AI-powered system within the CYLCOMED toolbox that monitors network traffic in real time to detect anomalies indicating cyber threats or malfunctions. It offers explainable insights into detected issues, integrates seamlessly with other CYLCOMED tools like LOMOS, and supports scalable deployment across various healthcare environments using Docker and Kubernetes.

Connected Medical Devices and Services Management Tools

This component focuses on reducing the attack surface of medical devices by creating a secure channel between the OTA Mechanism Management Server, application repositories, and medical devices. It scans application updates for vulnerabilities before deploying them, ensuring only secure updates reach active device partitions. The architecture includes a fleet of medical devices, a Mender Server with various microservices for update management and authentication, and a workstation that prepares and triggers update artefacts.

Self-Sovereign Identity solution (Lus4MED)

LuS4MED is a decentralised authentication system based on Self-Sovereign Identity (SSI), giving users full control over their data and credentials. Within the CYLCOMED project, it enables secure user authentication for accessing patient data. The system includes two components: an Agent that integrates SSI with the Hospital Information System, acting as both credential issuer and verifier, and a Mobile App where users store and manage their credentials for authentication during sign-up and login processes.

Authorisation solution C-OPA

This component is a security proxy for the FE4MED system, consisting of three parts: (1) Envoy Proxy, which handles incoming requests and forwards them for evaluation; (2) OPA (Open Policy Agent), which checks requests against security policies written in Rego, mainly validating JWT tokens and user permissions; and (3) a Policy Store, where bundled security policies are stored and periodically retrieved by OPA.

Data Protection solution (FE4MED)

FE4MED is an advanced data encryption solution that secures patient data during storage and sharing, using Cyphertext-Policy Attribute-Based Encryption (CP-ABE). It enables fine-grained

Funded by Horizon Europe Framework Programme of the European Union

access control by encrypting data with attribute-based policies, allowing only users with the correct attributes to decrypt and access the information.

Connected Medical Device integrity check tool

The implemented CYLCOMED tools have been integrated into a multi-parameter monitor designed for closed-loop neuromuscular relaxation control. Therefore, it is responsible for measuring neuromuscular relaxation, calculating the drug dose to be injected to maintain the level at a specific value, and then autonomously controlling an infusion pump to administer the drug.
In the real world, medical data is often exported to external cloud systems (HIS systems and similar). Therefore, the device operates in a hyper-connected environment, and this is where the tools and technologies developed throughout the CYLCOMED project come into play.
As can be presumed, modifying a medical device is a complex task with numerous implications regarding both security and regulations. Additionally, medical devices typically lack sufficient power to run the developed tools or don't have an operating system that allows their execution. For all these reasons, the chosen approach is to use an external device that connects directly to the monitor, integrating all the tools, and acting as the intermediary between the monitor and the external world. In this case, a Raspberry Pi 4 mini-computer was used, which has sufficient power for deploying the applications that comprise the CYLCOMED toolbox, as well as the necessary communication ports.

Security Dashboard

The CYLCOMED security Dashboard is a centralized platform that collects and visualizes security data from the CYLCOMED toolbox to provide real-time awareness of threats and risks related to connected medical devices (CMDs). It supports hospital IT teams by aggregating logs and alerts (e.g., from LADS and LOMOS), analysing risk levels, displaying intuitive visual insights, issuing real-time alerts, and integrating seamlessly with other CYLCOMED tools for a comprehensive cybersecurity overview

CYLCOMED Toolbox: Risk management tool

The CYLCOMED framework is a methodological approach designed to enhance the cybersecurity of healthcare services utilizing connected medical devices (CMDs). This framework aims to safeguard patient data and minimize risks associated with CMD vulnerabilities by addressing outdated operating systems, hardcoded credentials, weak authentication mechanisms, and limited resources. The CYLCOMED framework consists of several phases: data flow diagram decomposition to visualize data flows and storage components; cyber kill chain analysis to identify potential threat vectors and implement cybersecurity controls at critical stages; cybersecurity controls selection based on the analysis results; functionality impact analysis to assess impacts on CMD benefits and identify new hazards; and a final decision-making process to determine the safety and security of the CMD, implementing necessary measures accordingly. Deliverables include a risk benefit scheme, data flow diagram decomposition analysis, cyber kill chain threat modelling results, cybersecurity controls implementation guidelines, and an assessment of benefits versus implemented controls impact.

Funded by Horizon Europe Framework Programme of the European Union

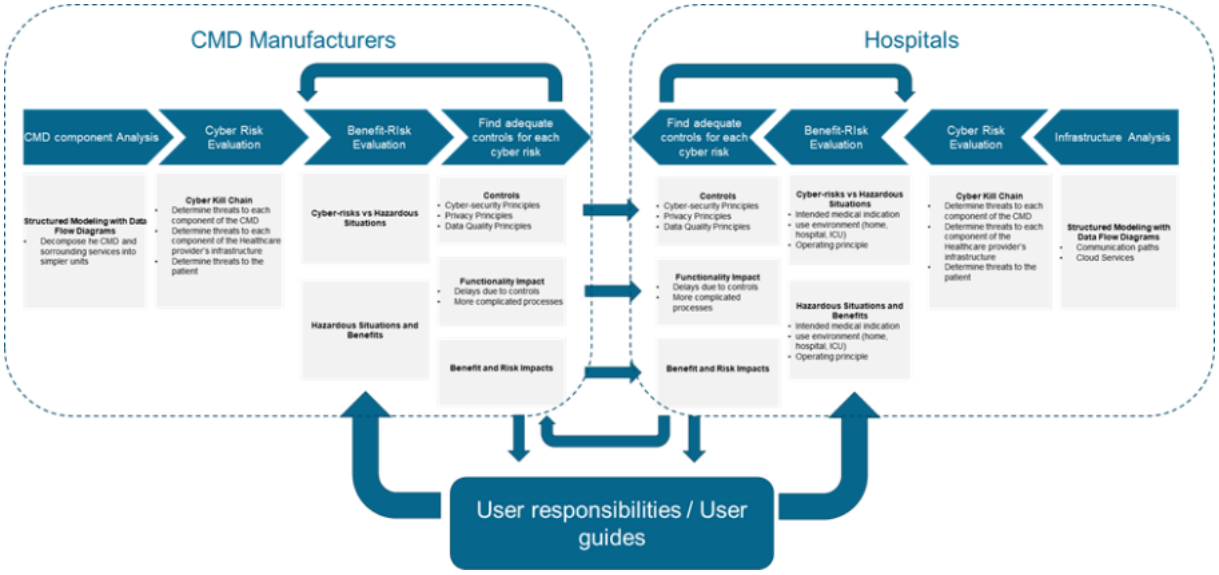

Figure 1: Risk management framework overview

As described in D4.3, the tool developed by INOV, helps in evaluating and mitigating cyber risks related with NMT signal simulator, external module and infusion pump of Pilot 1, and to address data privacy concerns of hospital scenarios of Pilot 2.

Moreover, a generic Risk Management Tool, enabling the use of any risk framework, was developed, enabling stakeholders, including manufacturers, hospitals, and patients, to collaboratively identify threats, assess vulnerabilities, and evaluate risks through a structured, modular interface. It supports risk-benefit analyses by mapping cybersecurity controls to device functions, assessing their potential impact on safety and performance.

Its key functionalities are:

- Asset, threat, and vulnerability management;
- Risk assessment, evaluation, and treatment planning;
- Visualization of risk levels and control effectiveness;
- Role-based Dashboards for different stakeholders;
- Integration with hospital and manufacturer processes.

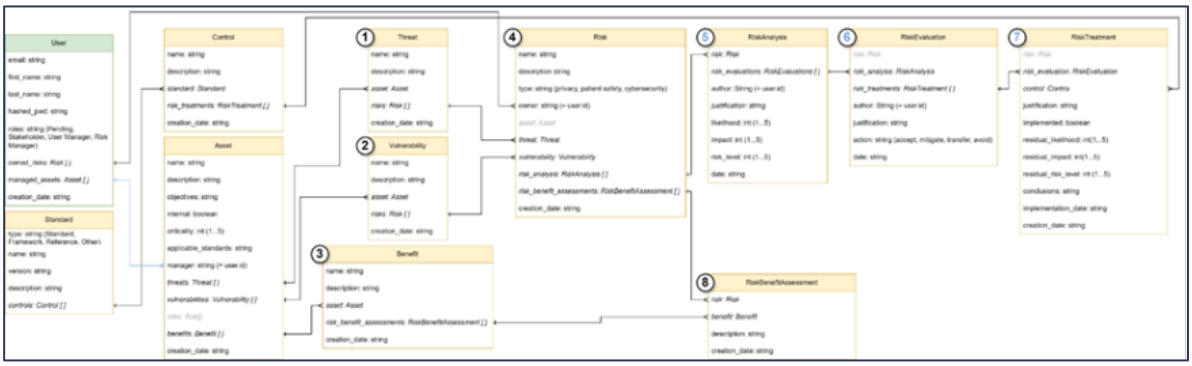

Figure 2: Risk Management Tool data model

Funded by Horizon Europe Framework Programme of the European Union

Figure 3: Risk management tool Dashboard showing one risk treatment impact on risk

2.2 Pilot 1 - Hospital Equipment: activities performed

The developed tools ensure secure oversight of Connected Medical Devices, keeping them updated with the latest security patches and preventing vulnerabilities from flawed configurations. Security scans are conducted before deployment to detect known issues. Components from the CYLCOMED toolkit have been deployed using these tools.

Medical device certification is complex and time-consuming. The strategy has involved integrating CYLCOMED security features into a Linux-based board that connects to legacy devices via a serial channel, maintaining essential functionalities while safeguarding against cybersecurity risks. This board communicates vital patient data to other medical devices and the web server mimicking the behaviour of the Hospital Information System (HIS) via Ethernet, adhering to regulatory security standards. It leverages a legacy device (Vision Air) for ICU scenarios.

Upgrading other devices requires an integration kit and protocol for generating cybersecurity alarms. Manufacturers must adapt the external board with an open protocol from CYLCOMED. A User Guide details the connection and communication protocol for the Vision Air multi-parameter monitor and includes specific alarms for proper integration.

The strategic focus has been to incorporate in the system some essential functionalities that optimize service delivery, ensure security, and enhance efficiency:

- Ensure secure updates for medical device services.
- Reduce the attack surface for medical devices and cloud infrastructure.
- Detect configuration issues.
- Guarantee software and configuration integrity.

2.2.1 Software tools implementation in Pilot 1

Live Anomaly Detection System (LADS)

During this M24-M36 period, we have finalised the integration with LADS to complete the ingestion pipeline for AI-driven anomaly detection. For this purpose, the Dashboard has been deployed and ensured full deployment in the RGB testbed, using Ansible for automated

Funded by Horizon Europe Framework Programme of the European Union

provisioning. Pilot Testing has taken place to validate Dashboard performance in real-world conditions and refine detection algorithms.

Data from LADS (network-level anomalies) has been analysed together with LOMOS (system log anomalies), helping detect attack patterns. The results are presented in the Dashboard.

To ensure seamless integration, the Dashboard has been deployed alongside LADS and LOMOS, using automation tools such as Ansible. This ensures:

- Consistent and reliable deployment across environments.
- Standardised data ingestion mechanisms to collect security insights from all relevant sources.
- Automated updates and scalability to accommodate additional security tools in the future.

Log Monitoring System (LOMOS)

As reported in D5.3, LOMOS architecture has been finalised and its functionalities fully developed by M33. During the M24-M36 period, we have finalized the integration with LOMOS in order to complete the ingestion pipeline for AI-driven anomaly detection. For this purpose, LOMOS has been deployed alongside LADS and the Dashboard on the EVIDEN cloud that is connected with the RGB testbed, using manual deployment and also IaC (Ansible) for automated provisioning.

Pilot Testing has taken place to validate LOMOS performance in real-world conditions and refine detection algorithms by ingesting application logs from the Lus4MED and FE4MED components on the RGB server in the RGB testbench, run model training and display the anomaly score (JSON format) on the Dashboard. LOMOS and Dashboard are integrated through LOMOS API-2.

The decision to deploy LOMOS on the EVIDEN server was influenced by the fact that LOMOS needs GPU power to train the model which RGB server can't provide.

Connected Medical Devices and Services Management Tools

The implementation of Mender has played a crucial role in minimizing the attack surface of medical devices. It achieves this objective by consistently updating software and effectively managing security patches, thereby ensuring robust functionality and safeguarding against potential vulnerabilities.

The setup and implementation of Mender, has included the registration of 2 medical devices (plus any arbitrary device of a compatible architecture) and the generation of artefacts to be securely uploaded to said registered devices. It is now functional in a controlled demo environment. Documentation for the process of deploying the components has been finalised.

The Mender setup is currently functional in its controlled environment. To further expand what Mender can deploy, new artifacts must be generated, which in turn requires a containerized application deployed from Docker images for example.

Self-Sovereign Identity solution (Lus4MED)

This component has been deployed in RGB premises. During the period M24-M36, RGB has integrated the VC issuing process for user registration, using the LuS4MED mobile app. Also, the integration of verifiable presentation for user login, has been addressed with the support of Eviden development team. Several meetings have taken place for easing both integration process. Once these processes have been performed, RGB has integrated the C-OPA authorisation tool.

Funded by Horizon Europe Framework Programme of the European Union

We have developed a decentralised and user-focused solution for safeguarding identity management (SSI solution for user authentication, named LuS4MED. We have carried out the development of several web components, particularly those that enable the visualization of patient measurements that are stored in an encrypted format within the database. We have integrated core components for user registration and authentication (LuS4MED). This integration supports secure access.

The LuS4MED makes use of the agent (LuS4MED Agent) to generate the verifiable credential (VC) based on the information provided by the hospital, verify the credentials presented by the user and interact with the hospital for integrating the SSI mechanisms. A mobile app (LuS4MED mobile app) is used for storing the user VCs, allowing the user interaction with the hospital system for authentication purposes.

The implementation includes the flow for issuing a credential during the user registration process and the presentation of the user credentials during the login process, for accessing the hospital system and therefore the patient's data.

Authorisation solution C-OPA

We have developed a decentralised and user-focused solution for controlling access to prevent unauthorized use (authorisation solution, named C-OPA). We have carried out the integration of C-OPA from Martel, which has been placed between the server and the decryption tools.

Martel has provided an authorisation solution named C-OPA described in section of D5.2. The simulated Hospital Information System (HIS) has created the environment needed for registering the user (medical staff) providing a web interface where the user enters their data required by the HIS. Martel has worked with RGB to deploy the component and create a configuration and set of policies to protect the FE4MED component specifically, alongside token verification with LuS4MED.

Data Protection solution (FE4MED)

The FE4MED tool has been deployed and running in this pilot. The encryptor module deployed on the RPI stores the policies needed for encrypting the patient data provided by the CMDs connected to the RPI. These encrypted data are sent to the HIS and stored safely and decrypted by FE4MED server when requested by the medical staff. The complete flow for encrypting and decrypting patients' data has been tested and works in a smooth manner We have implemented a secure and privacy solution for transferring data between devices and healthcare providers across different platforms, by using innovative encryption methods (ABE solution, named FE4MED).

In the M24-M36 period, we have finalized the integration along with the RGB medical features. That is, the SW component for the encryption tools provided by EVIDEN into both the server and the RPI for the FE4MED component. This allows patient data collected by VisionAir to be sent encrypted to the server using appropriate policies. On the server, data is stored encrypted in a database once it is uploaded.

Basically, the data collected by the CMDs are protected by encrypting the patient's data with the ABE solution and are stored in the web service simulating the hospital system. When the medical staff accessing the hospital system through the SSI App (LuS4MED mobile app) and request the encrypted patient's data, present their user attributes. Then, the FE4MED decrypts those data (based on the user attributes) the user is allowed to see. The use of the data

Funded by Horizon Europe Framework Programme of the European Union

protection layer is monitored by the AI-Log monitoring tool (the LOMOS solution previously described.

In the following image, details are shown regarding the log messages generated, highlighting the encryption of data within the EVIDEN tools before its transmission to the server

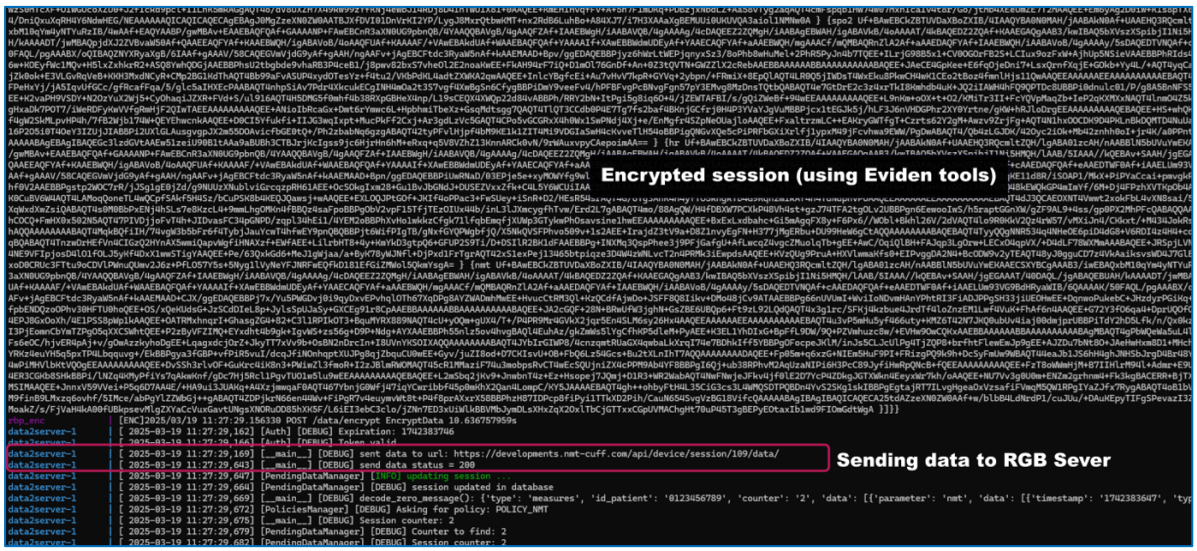

Figure 4: Log messages generated, encryption with EVIDEN tools and transmission to the server

Connected Medical Device integrity [RGB]

RGB`s main tasks in the M24-M36 period have been to complete the integration with the user registration and authentication components. We have also completed the web platform for data visualization.

The completion of these steps has been key to enhance the robustness and security of the overall system, contributing to a more effective and secure medical device management framework. The close collaboration with EVIDEN has been crucial in ensuring that all components function cohesively and meet the designated security standards for deployment.

The developments concerning the VisionAir and its communication with the pumps through the Raspberry Pi (RPI) external board have been completed, including some necessary adjustments and tests after the ongoing integrations. So, the system is able to measure the NMT, calculate the dose to infuse and finally order the correct infusion to pumps.

This ensures that RGB part of the integration has been ready to test all cybersecurity tools to facilitate a smoother user experience, thus enhancing the overall functionality of the system.

CYLCOMED Security Dashboard

During the M24-M36 period, the Dashboard has integrated LADS and LOMOS to monitor cybersecurity anomalies detected in the testbed infrastructure.

The focus has been on evaluating the interaction between network anomalies and log-based security insights. Data from LADS (network-level anomalies) and LOMOS (system log anomalies) has been analysed together, helping detect attack patterns.

In Pilot 1 (RGB), the Dashboard was successfully deployed in a hybrid setup. LADS, LOMOS, and the Dashboard ran in the EVIDEN cloud, while RGB operated the testbed on-premises. The two environments were linked over secure network channels (dedicated VPNs), allowing telemetry and alerts to flow reliably without exposing hospital systems. This hybrid setup

Funded by Horizon Europe Framework Programme of the European Union

enabled fast iteration and scaling in the cloud while keeping device-side operations and test signals under RGB's control.

2.2.2 Risk assessment tool implementation in Pilot 1

The CYLCOMED Risk Management Framework was followed through, with publicly available information regarding pilot 1 and the results presented here are a synthesis of the systems involved.

A simplified version of the dataflow diagram (DFD3 format) can be found below.

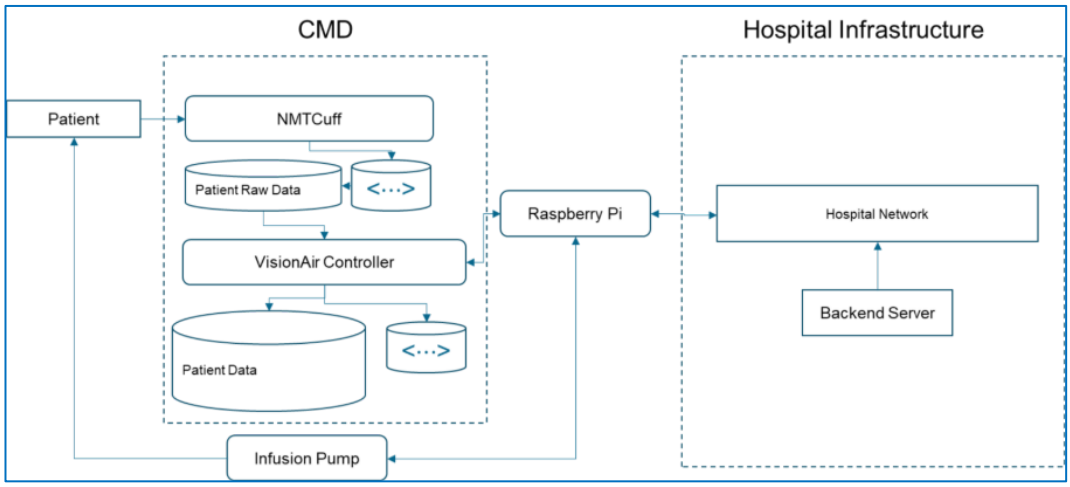

Figure 5: Dataflow diagram for Pilot 1

As illustrate in the dataflow diagram, the cyber kill chain analysis was performed and a sample of it can be found in the next table, along with the risk analysis result (likelihood and impact).

Path	Kill-chain phase	Asset / Component	Risk ID	Risk Name	Risk Description	Likelihood (1–5)	Impact (1–5)
1	Recon	Single-Board Computer (SBC) – Raspberry Pi	R1	Foothold on bedside host → pivot into ICU LAN.	Compromise of the SBC gives the attacker a launchpad to move laterally and observe/modify traffic.	3	4
1	Delivery	Single-Board Computer (SBC) – Raspberry Pi	R5	Backdoored image gains persistent code-exec.	Long-lived bedside compromise with ability to alter data/commands.	3	4
1	Exploit	Single-Board Computer (SBC) – Raspberry Pi	R9	Weak SSH/services allow bedside takeover.	Attacker gains command execution and can pivot or tamper with control traffic.	3	4
1	Install	Single-Board Computer (SBC) – Raspberry Pi	R19	Offline media access / rogue peripherals persist.	Long-term persistence with ability to pivot and subvert data/commands.	3	4
1	C2	Single-Board Computer (SBC) – Raspberry Pi	R21	Remote tasking/exfil via DNS/HTTPS under thresholds.	Ongoing attacker control with stealthy data leakage from edge.	3	4

Table 1: sample of the Cyber Kill chain analysis for pilot 1

Funded by Horizon Europe Framework Programme of the European Union

Then the cybersecurity controls were mapped to the risks.

Kill-chain path	Risk ID	Risk Name	Control name	Comp.	How it mitigates (L – likelihood, I – Impact)	Control Description	Res. Likelihood	Res. Impact
1	R1	Foothold on bedside host → pivot into ICU LAN.	Integrity – Change & Configuration Management	MENDER	Use: enforce desired-state, close unused ports, deploy only signed builds, auto-rollback. L/I: L↓ attack surface & drift; impact unchanged.	MENDER – enforce desired-state, close unused ports, deploy only signed builds, auto-rollback.	2	4
1	R1	Foothold on bedside host → pivot into ICU LAN.	Incident Detection & Reporting	LADS	Use: edge sensor flags scans/banners. L/I: L↓ via rapid block/triage pre-exploit.	LADS – edge sensor flags scans/banners; rapid block/triage pre-exploit.	2	4
1	R1	Foothold on bedside host → pivot into ICU LAN.	System & Network Logging	LOMOS	Use: forward auth/daemon logs with unique timestamps. L/I: L↓ by revealing reconnaissance early.	LOMOS – forward auth/daemon logs with unique timestamps to reveal recon early.	2	4
1	R5	Backdoored image gains persistent code-exec.	Integrity – Change & Configuration Management	MENDER	Use: verify signatures, staged rollout, health-checks + rollback. L/I: L↓ blocks untrusted images.	MENDER – signed images, staged rollout, health-checks, rollback to block untrusted images.	2	4
1	R5	Backdoored image gains persistent code-exec.	Integrity – Digital Signatures & Logging	MENDER / LOMOS	Use: sign artifacts; log provenance & results centrally. L/I: L↓ (harder to insert rogue code); I↓ via auditability.	MENDER/LOMOS – signed artifacts with central provenance logs.	2	4
1	R5	Backdoored image gains persistent code-exec.	Integrity – Tamper Detection & Integrity Monitoring	Device Integrity Check	Use: attest SBC state; block operation on integrity “red.” L/I: I↓ stops trusted use after compromise.	Device Integrity Check – attest SBC state and block on integrity “red.”	2	4
1	R9	Weak SSH/services allow bedside takeover.	Integrity – Change & Configuration Management	MENDER	Use: enforce hardened baseline; disable password auth; close mgmt endpoints. L/I: L↓ removing	MENDER – hardened baseline, no password SSH, closed mgmt endpoints.	2	4

Funded by Horizon Europe Framework Programme of the European Union

					easy entry points.			
1	R9	Weak SSH/services allow bedside takeover.	Continuous Log Monitoring	LOMOS	Use: alert on repeated SSH failures/new processes/su. L/I: L↓ via immediate response.	LOMOS – alerts on repeated SSH failures/new processes/su.	2	4
1	R19	Offline media access / rogue peripherals persist.	Integrity – Tamper Detection & Integrity Monitoring	Device Integrity Check	Use: continuous integrity attest; fail-closed posture. L/I: I↓ prevents trusted operation while compromised.	Device Integrity Check – continuous attestation, fail-closed.	3	3
1	R19	Offline media access / rogue peripherals persist.	Availability – Incident Response & Recovery	Dashboard / MENDER	Use: remote quarantine & re-image/restore. L/I: I↓ by minimizing time/impact.	Dashboard/MENDER – remote quarantine and re-image/restore.	3	3
1	R21	Remote tasking /exfil via DNS/HTTPS under thresholds.	Incident Management - Incident Detection & Reporting	LADS	Use: egress modelling & beacon detection. L/I: I↓ via quick block of C2 paths.	LADS – egress modelling and beacon detection to block C2.	3	3
1	R21	Remote tasking /exfil via DNS/HTTPS under thresholds.	Logging & Monitoring - Continuous Log Monitoring	LOMOS / Dashboard	Use: correlate host/user timelines; escalate case. L/I: I↓ by shortening attacker dwell time.	LOMOS/Dashboard – correlate host/user timelines; escalate and contain.	3	3

Table 2: sample of the cybersecurity controls attribution and analysis from the cyber kill chain analysis

And the final Benefit-Risk Assessment was made.

Asset	Benefit	Risk	Risk ID	Why this pairing	Key CYLCOMED controls (how)	Verdict (benefit vs residual risk)
Single-Board Computer (SBC) – Raspberry Pi	Faster closed-loop response	Foothold on bedside host → pivot into ICU LAN.	R1	Bedside control improves response but exposes edge services.	MENDER hardens/locks baseline; LADS flags scans; LOMOS central auth/process logs; Dashboard triage.	Outweighs (high safety gain; residual medium, monitored).

Funded by Horizon Europe Framework Programme of the European Union

Single-Board Computer (SBC) – Raspberry Pi	Rapid hardware recovery	Backdoored image gains persistent code-exec.	R5	Frequent swaps/rollouts heighten supply-chain risk.	MENDER signed/staged updates and rollback; Device Integrity Check post-swap attestation; Dashboard IR.	Outweighs (availability win; update integrity enforced).
Single-Board Computer (SBC) – Raspberry Pi	Remote administration and troubleshooting	Weak SSH/services allow bedside takeover.	R9	Operational teams need remote access, but exposed SSH or default services can be abused for takeover.	MENDER enforces hardened baseline, disables password auth, and closes management endpoints; LOMOS alerts on repeated SSH failures and suspicious new processes.	Outweighs (operational manageability preserved; residual compromise risk medium and closely monitored).
Single-Board Computer (SBC) – Raspberry Pi	Field serviceability and swappable hardware	Offline media access / rogue peripherals persist.	R19	Bedside units must be physically accessible, which increases risk of offline modification or rogue devices.	Device Integrity Check provides continuous integrity attestation and fail-closed posture; Dashboard / MENDER support remote quarantine, re-image, and restore.	Outweighs (serviceability and cost benefits; residual physical-persistence risk moderate but bounded by attestation and recovery).
Single-Board Computer (SBC) – Raspberry Pi	Remote support and telemetry over standard protocols	Remote tasking/exfil via DNS/HTTPS under thresholds.	R21	Standard web protocols are needed for interoperability, but they can hide stealthy command-and-control.	LADS egress modelling and beacon detection; LOMOS / Dashboard correlate host and user timelines and escalate suspicious cases.	Outweighs (interoperability and observability benefits; residual covert C2 risk medium and actively monitored).
Backend patient-data DB & access layer	Discoverable API surface for integration	Object patterns gleaned for later IDOR.	R4	Integration and self-service queries require stable, predictable APIs, which also aid attackers in mapping objects.	LADS detects high-rate 404s and ID walks at ingress; LOMOS keeps verbose subject/object/action API logs to spot guessing and recon.	Outweighs (integration and automation gains; residual recon risk medium–low and monitored).

Table 3: sample of the benefit risk analysis performed on pilot 1

These data were fed into the risk management tool as can be seen in Figure 6, Figure 7, and Figure 8.

Funded by Horizon Europe Framework Programme of the European Union

Figure 6 Risk Management Tool showing the risk analyses Dashboard for Pilot 1

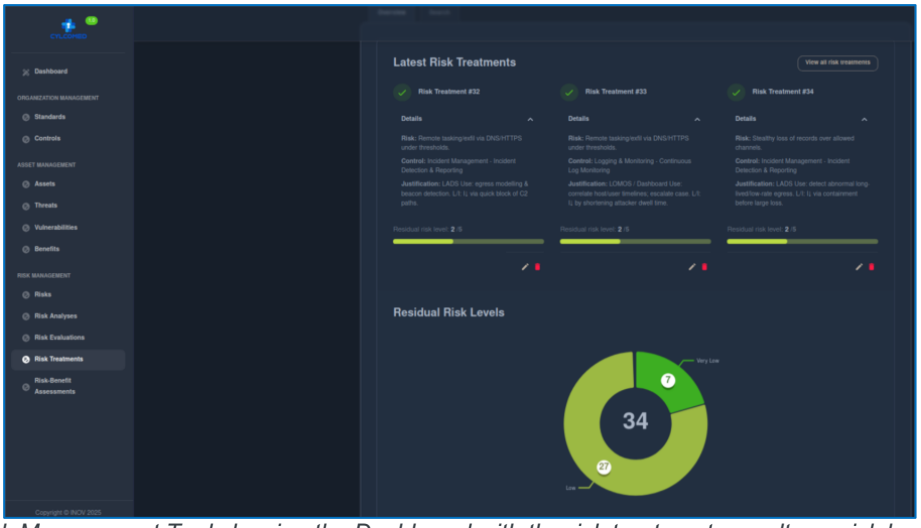

Figure 7: Risk Management Tool showing the Dashboard with the risk treatments results on risk levels for Pilot 1

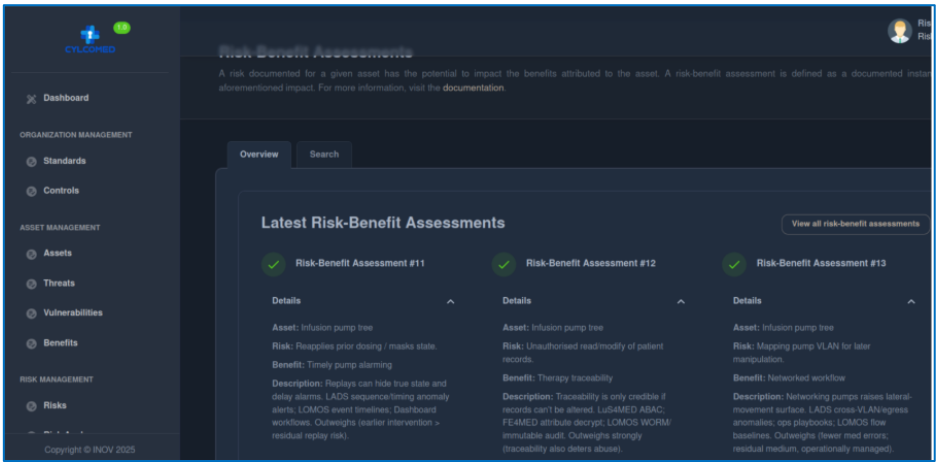

Figure 8: Risk Management Tool showing the Dashboard with the benefit-risk assessment for Pilot 1

Funded by Horizon Europe Framework Programme of the European Union

2.3 Pilot 2 – Telemonitoring platform: activities performed

Pilot 2 exploited the different deployments and subpilots to investigate as much as possible toolbox applicability in real scenarios and collect the greatest number of feedback, ensuring to maximize the outcomes from the consortium diversity.

2.3.1 Deployment A and deployment B

Deployment A experience focused on the real-world complexity, in this deployment the three hospitals involved in the consortium tested different aspects of CYLCOMED toolbox, investigating actual requirements, restriction and complexity.

Real patients were involved in the framework of a clinical trial; volunteers and clinicians were also involved to provide a complete overview.

In this deployment both patient (n. 12) and volunteers (n. 12) used the medical devices provided by MCI to monitor their physiological parameters on premises and outside (at home, on emergency vehicles). The next section will detail the Clinical Trial procedures used for patient enrolment. The volunteers used the different sensors during a week to test their usability. Each volunteer was given a mobile phone which was preconfigured by MCI to connect only to the server in their premises using any available internet connection. The medical devices used Bluetooth technologies to connect to one of the mobile phones. Different strategies were adopted in the different deployments to ensure that clinical data were adequately protected. The measures vary depending on the deployment site (e.g. real patients' data were stored on premises in a dedicated installation) During the last period of the deployment A, the IT department of the hospitals could watch the Dashboard Tool for security issues.

Deployment B was a controlled environment where no human data were collected. This deployment was crucial to integrate the different tools in the telemonitoring platform and to allow a safe space for testing and evaluating performances to all the technical partners. some simple cybersecurity attacks (e.g brute force attack, dictionary attack, slow DOS attack) were also simulated to test LOMOS. Integrations with the Lus4Med and Fe4Med tools were also tested and validated in this deployment.

Clinical trial procedures

In this section are reported the details of the clinical trial that allowed to enroll real patients and gain usefull insights from the patients about the CYLCOMED project.
The study consisted in a post-marketing investigation with a medical telemonitoring system in paediatric and young adult patients affected by heart failure (HF) due to complex congenital heart disease (CHD) ≥16 years. These patients underwent surgical interventions leading to a univentricular blood circulation (Fontan Circulation) leading to frequent exacerbations and hospitalizations. Due to the high rate of cardiovascular (CV) adverse events in this population, the recurrent need for hospitalisation and therapy adjustments and the reduced life expectancy, the HF-CHD population benefits the most from remote telemonitoring. Patients were enrolled among those admitted into the hospital ward or in Day Hospital after a detailed explanation of the study and signature of the informed consent.
The telemonitoring system combines Class I and Class II medical devices and associated Class I digital monitoring platform, including 1-lead ECG, an oximeter, an infrared thermometer, a sphygmomanometer and a weighting scale. In addition, the clinical technician called the patient every workday during the 1st week and every 2 weekdays after the 1st week of monitoring, to assess symptoms, compliance and any other technical issue.

Funded by Horizon Europe Framework Programme of the European Union

The clinical study was conducted from January to November 2025. A total of 12 patients (7 males, 5 females) has been enrolled, mean age 20.4 years old (range 16–28-year-old). The patients were asked to wear the telemonitoring top to record the 1-lead ECG for at least 6 hours per day and to use daily the other connected medical devices (an oxymeter, an infrared thermometer, a sphygmomanometer and a weighting scale) and to do not leave more than 3 days without any use of the telemonitoring system.

Three patients had an early stop of the monitoring, due to anxiety induced by the monitoring, to a rupture of the textile top during physical activity, and for logistic reason (summer holidays and travelling). The telemonitoring was clinically useful in 45% of patients:

- The clinicians identified a case of non-adherence to pharmacological therapy of a patient in the active list of heart transplant and prompt correction with an active counselling on the importance of adherence to optimized medical therapy;
- The clinicians increased the pharmacological anti-arrhythmic therapy due to the presence of supraventricular arrhythmias at the 1-lead ECG monitoring, not always perceived as palpitations by the patient;
- The clinicians reduced the pharmacological therapy due to hypotension and desaturation in another patient;
- The clinicians identified unexplained ECG changes during tachycardia requiring additional exams (stress ECG), which did not reveal particular CV abnormalities at peak effort;
- The clinicians reassured a patient that no ECG changes or arrhythmias were detected when the symptom was present (palpitations).

No mortality or major CV adverse events happened during the telemonitoring.

The clinicians expected to include 16 patients in the study, but only 12 patients were enrolled. A total of 9 additional eligible patients were screened and refused to participate for the following reasons:

- Logistics, the patient was travelling alone or had a planned trip and did not want to bring the telemonitoring system (3 patients)
- Perceived anxiety during the 24-hour Holter monitoring, so not willing to undergo a 2-month telemonitoring study (2 patient)
- Conflicting willing of participating between adolescent patient and his/her caregiver, perceived as an additional duty by the caregiver (reduced independency of the patient) (2 patients)
- Not interested in being part of a clinical research (2 patients).

Challenges faced during the implementation of digital health tools in the clinical workflow:

The monitoring activities and the concomitant collection of data for the cybersecurity evaluation were performed continuously, although some challenges emerged, mainly related to the performance and usability of remote monitoring devices and relevant to the clinical interpretation of monitored signals.

Key issues and corresponding solutions included:

- **Respiratory rate inaccuracies:** The wearable sensor-embedded t-shirts often produced artefact-ridden data, at times falsely suggesting critical events. The manufacturer attributed this to incorrect sensor positioning and signal disruption when patients talked. New t-shirt sizes were supplied to improve fit and sensor placement.
- **Limited ECG usability:** The MCI Dashboard initially provided only brief ECG displays, restricting cardiologists to qualitative rather than precise quantitative interpretation. MCI

Funded by Horizon Europe Framework Programme of the European Union

increased the temporal dimensions of the ECG trace displayed, ensuring continuity in the signal shown to the clinicians.

- **Pulse oximetry errors:** The oximeter sent readings before stabilizing, generating inaccurate values that remain permanently stored and could not be excluded from exported datasets, potentially compromising data quality. The interpretation of the first signals was made considering this limitation. MCI then has increased the stabilization time of the sensor, which sends the data after 30 seconds of measurement (value validated by the clinicians).

- **Blood pressure cuff sizing:** The standard cuff provided was too large for paediatric use. New devices with appropriate cuff size were provided.

In the protocol the textile top was required to be used at least 6 hours per day. The clinicians also provided instructions on how to wash it by hand or in a washing machine with a gentle program at 30°C and how to charge the electric unit of the 1-lead ECG device and the smartphone. Failing of a correct charge of the devices or too much physical distance of the smartphone from the connected medical devices impaired the recording.

Anxiety is common in patients with HF-CHD with a higher prevalence than in the general population. This is caused by factors like uncertainty about their health, the burden of ongoing medical care, fear of reinterventions, functional limitations, and the long-term psychological impact of living with a chronic condition.

These challenges highlight the complexity of implementing digital health tools in real clinical environments. They underscore the need for early, continuous collaboration between clinicians and technical partners, transparent communication, and thorough validation to ensure technology is clinically meaningful, scalable, and beneficial for patients.

2.3.2 Software tools implementation in Pilot 2 (Deployment A and B)

Pilot 2 has provided the possibility to get insights on all the tools, giving valuable feedbacks to tech partners and tech providers, allowing a better understanding of limitations and requirements for tools that have the ambition to be hospital-deployable.

Live Anomaly Detection System (LADS) and Log Monitoring System (LOMOS)

LADS has been deployed and operating since the start of Pilot 2 on a dedicated OPBG server inside the hospital. All flow telemetry, model training, and inference are processed entirely within the hospital network. In line with the pilot's security constraints, day-to-day access and operations were delegated to MCI. To support this model, LADS was engineered for semi-automatic deployment and near-zero routine maintenance: the stack runs in Docker via docker-compose, and its execution mode is set through environment variables—training for model learning and inference for live detection. The CYLCOMED Dashboard is integrated with LADS on the same environment, which made it straightforward to review detected anomalies, inspect explainability outputs, and confirm effectiveness during the OPBG iterations.

The LADS tool combines sensors and an "AI brain" connected via RabbitMQ, enabling ingestion and parallel model execution. The current architecture of LADS detaches sensors from the brain, facilitating scalability. On-premise operator-triggered training automates model roll-out to inference. The Dashboard, bundled with LADS, views, flow tables, feature-importance, and source/destination breakdowns to help analysts validate detections

Because of the pilot's nature and strict security controls to protect data and clinical work, we had limited context about the environment. This made it hard during inference to decide if a

Funded by Horizon Europe Framework Programme of the European Union

network flow was truly anomalous. We resolved this in the analysis phase through joint review sessions with OPBG's cybersecurity team, mapping allowed services and refining labels. As a result, we could clearly separate real anomalies from normal traffic and reduce false positives.

In Pilot 2, LOMOS is containerised using Docker and deployed on the dedicated machines with GPU (server) that serve as the testing platform for the Toolbox in hospitals. In this scenario, LOMOS consumes the MHP (Mediaclinics Health Platform) reverse proxy logs, trains the model using these logs, runs the inference and displays the anomaly score on the Dashboard. LOMOS is integrated with the Dashboard by exposing LOMOS API-2.

Due to highly secure environment in the OPBG hospital, LOMOS deployed there it was not possible to run despite several attempts and modifications to its configuration. On the other side, on the NUC used to collect data from volunteers, hosted in MCI facilities, LOMOS was also deployed and there was no issue accessing (using SSH) and running it. For the validation, the data (logs) were manually transferred to another instance of LOMOS running in XLAB premises where the model was trained. The model results are displayed on the Dashboard through LOMOS API-2.

Challenges faced during the development and deployment:

Medical environments where LOMOS is deployed are heterogeneous and with different limitations regarding hardware available (GPU present or not), virtualisation and hostOS technologies used as well as permissions to run software. Thus, it was necessary to reconfigure LOMOS deployment scripts to have it successfully deployed and running in these environments. This involved adding Nvidia CUDA driver bindings to the LOMOS Pytorch version to enable compatibility with Nvidia GPUs on the host server, alleviating the need to separately install CUDA drivers, and resolving LOMOS containers communication issues in the same Docker network (no need now to call the host IP address).

Despite these improvements, there were still issues in running LOMOS in the OPBG hospital due to restrictions on executing necessary LOMOS dependencies in a restrained hospital environment. However, this was not an obstacle to validate LOMOS as reverse proxy logs from the MHP (Mediaclinics Health Platform) were manually exported to similar instance of LOMOS running at XLAB premises and the model was trained locally. The anomaly scores were exposed to the Dashboard by calling LOMOS API-2.

CSelf-Sovereign Identity solution Lus4MED

During the period M24-M36 the LuS4MED component has been initially deployed in MCI VM. This deployment has been replicated on the 3 different hospital environments. MCI Healthcare Platform (MHP) has integrated this component for VC issuing and validation with the aim of user registration and login processes. A LuS4MED mobile app has been used to this end. The integration of Lus4MED has been addressed with the support of EVIDEN development team. The MCI platform authorisation method (Keycloak) has been used for generating the initial access token needed for stablishing a trusted interaction between LuS4MED and the MHP system, for allowing the user access to the permitted resources (patient's data). Several meetings have taken place for facilitating the integration process. MCI developed some web components for the interaction between the user mobile app and the LuS4MED component.

The LuS4MED makes use of the agent (LuS4MED Agent) to generate the verifiable credential (VC) based on the information provided by the MHP, verify the credentials presented by the user through the LuS4MED mobile app, and interact with the MHP for integrating the SSI mechanisms. The mobile app stores the user VCs, allowing the user interaction with the MHP for authentication purposes.

Funded by Horizon Europe Framework Programme of the European Union

The implementation includes the flow for issuing a credential during the user registration process and the presentation of the user credentials during the login process, for accessing the MHP and therefore MHP services, including the patient's data.

Data Protection solution FE4MED

The FE4MED tool has been deployed and running in MCI VM. During the period M24-M36 the LuS4MED component has been deployed and validated in MCI VM (Deployment B). The data to be protected by this tool are the questionnaire's answers the patients or the patient's caregiver fill in through the MCI mobile app. These answers are sent to the MHP platform through secure channels. The FE4MED encryptor, decryptor and key generation modules has been deployed on the MHP, besides the policies needed for encrypting the answers. These encrypted data are stored safely in the MHP and will be decrypted by FE4MED server when requested by the medical staff. The complete flow for encrypting and decrypting patients' data has been tested in the MCI VM.

When the users (the medical and admin staff) accessing the MHP system through the SSI App (LuS4MED mobile app) provide their attributes to the system. The access to the encrypted patient's data, will be allowed if the user attributes fulfil the policy used for encrypting the data. Then, the FE4MED decrypts those data (based on the user attributes) and the user is allowed to see those attributes permitted. The use of the data protection layer is monitored by the AI-Log monitoring tool (the LOMOS solution previously described).

CYLCOMED security Dashboard

The Dashboards were deployed in hospital dedicated on-premises servers. All collection, processing, and storage stay inside the hospital network in line with OPBG security policies. Day-to-day access and routine maintenance are delegated to MCI. The service is containerised (Docker + docker-compose) for low-touch operation; configuration is handled through environment variables to register data sources and enable/disable modules. Integration with LADS and LOMOS is complete: network and log anomalies are ingested in near-real time and shown through the standard views (time series, flow explainability, stacked bars, histograms, Sankey). During the pilot, alert thresholds and role-based views were tuned with OPBG's cybersecurity and clinical teams, and updates were rolled out during agreed maintenance windows to avoid any impact on clinical activity.

A key challenge was making the charts and tables truly useful for OPBG's cybersecurity team. Raw LADS/LOMOS outputs were informative but not always actionable: some views were too granular, others mixed sensitive fields, and several lacked the necessary context to determine whether to escalate, contain, or ignore an event. Dashboards were fine tuned with OPBG Dashboard to support decisions that protect data integrity and infrastructure security.

2.3.3 Risk assessment tool in Pilot 2 Deployment A

Risk assessment tool has been developed from scratches, based on the feedback from technical and clinical partners. Specifically, the relevant part for pilot 2 is the attention paid to the specific regulation that impact hospital workflow and procedures. While this tool was not tested directly in Pilot 2, the stakeholders in the clinics reviewed the tool and gave their feedback.In pilot 2, the CYLCOMED Risk Management Framework was also followed, and it's possible to find the simplified version of the dataflow diagram, the cyber kill chain analysis with the risk analysis as well, the risk mitigation table and the benefit-risk assessment made. Note that these tables are also samples from a broader analysis performed on pilot 2.

Funded by Horizon Europe Framework Programme of the European Union

DFD3 schematic

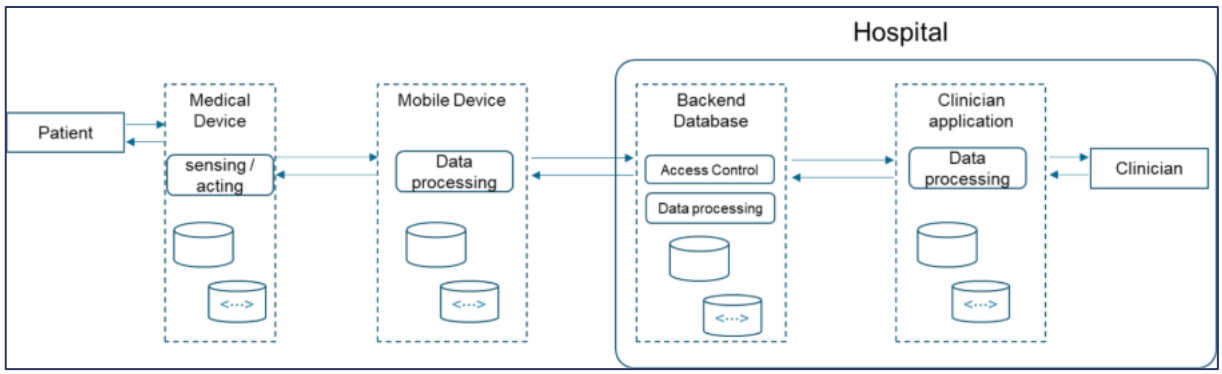

Figure 9: Dataflow diagram for Pilot 2

Cyber kill chain analysis

Path	Kill-chain phase	Asset / Component	Risk ID	Risk Name	Risk Description	Likelihood (1–5)	Impact (1–5)
1	Recon	Network / Ingress (API gateway)	P2-R1	Initial foothold at the gateway via known-vulnerability service.	Gateway compromise enables code execution and request manipulation on the gateway itself.	3	4
1	Delivery	Network / Ingress (API gateway)	P2-R19	Foothold without noisy scanning.	Code execution or logic bypass inside the gateway process.	3	4
1	Exploit	Backend (database & data-access)	P2-R11	Service-level compromise.	Privilege gain or data access in the processing service.	3	4
1	Install	Backend (database & data-access)	P2-R12	Keys enable mass access.	Bulk decryption or service impersonation using this layer's keys.	2	4
1	C2	Backend (database & data-access)	P2-R13	Persistent control inside service.	Remote tasking and data exfiltration from the processing service.	3	4

Table 4 Sample of the Cyber Kill chain analysis for pilot 2

Funded by Horizon Europe Framework Programme of the European Union

Controls

Kill-chain path	Risk ID	Risk Name	Control name	Comp.	How it mitigates : Use → L/I	Control Description	Residual Likelihood	Residual Impact
1	P2-R1	Initial foothold at the gateway via known-vuln service.	Incident Management - Incident Detection & Reporting	LADS	Ingress sensor flags scans/bruteforce; auto-block & case → L↓	Ingress Scan/Brute Detection & Block	2	4
1	P2-R1	Initial foothold at the gateway via known-vuln service.	Logging & Monitoring - System & Network Logging	LOMOS	Centralize WAF/HTTP/app logs; detect recon patterns → L↓	Centralized Web/API Telemetry	2	4
1	P2-R19	Foothold without noisy scanning.	Data Quality – Standardized Exchange	LOMOS	Safe parsers; reject-unknown schemas; quarantine failures → L↓+I↓	Strict Schema Validation (Reject-Unknown)	2	3
1	P2-R19	Foothold without noisy scanning.	Incident Management - Incident Detection & Reporting	LADS	Deserialization/RCE signatures at ingress; block → L↓	Ingress RCE/Deserialization Signatures	2	3
1	P2-R11	Service-level compromise.	Logging & Monitoring - Continuous Log Monitoring	LOMOS	Crash/priv-esc indicators; kernel messages; case raise → I↓	Runtime/Kernel Anomaly Alerts	3	3
1	P2-R12	Keys enable mass access.	Confidentiality - Data Classification & Encryption	FE4MED (KIA)	Tight issuance/rotation/revocation + audit → L↓	Key Lifecycle Governance	1	4
1	P2-R12	Keys enable mass access.	Logging & Monitoring - System & Network Logging	LOMOS	Monitor key-use/admin actions; alert anomalies → I↓	KMS Usage Auditing	1	4
1	P2-R13	Persistent control inside service.	Incident Management - Incident Detection & Reporting	LADS	Egress modelling; low-rate beacon detection; blocklists → I↓	Beacon/Egress Anomaly Analytics	3	3
1	P2-R13	Persistent control inside service.	Logging & Monitoring - Continuous Log Monitoring	LOMOS / Dashboard	Correlate timelines; orchestrate containment → I↓	Case Correlation & Containment	3	3

Table 5 Sample of the cybersecurity controls attribution and analysis from the cyber kill chain analysis for pilot 2

Funded by Horizon Europe Framework Programme of the European Union

Benefit-Risk assessment

Asset	Benefit	Risk	Risk ID	Why this pairing	Key CYLCOMED controls (how)	Verdict (benefit vs residual risk)
Device ingestion / API gateway	Request hygiene at the edge	Edge service exposure	P2-R1	Rate-limit and validation is beneficial but exposes services.	LADS scan/brute force detections & blocks; LOMOS central web/API logs; ops triage in Dashboard.	Outweighs (stability & quality gains; residual medium, monitored).
Device ingestion / API gateway	Consistent intake	Unsafe parsing/deserialization	P2-R19	Uniform interface can concentrate parser risk.	LOMOS strict JSON/FHIR schemas (reject-unknown); LADS RCE/deserialization signatures; Dashboard quarantine/patch.	Outweighs (interoperability gain; residual low-medium).
Stream processing & alerting	Deterministic calculations	Runtime CVEs	P2-R11	Determinism requires a secure runtime.	LOMOS kernel/runtime anomaly alerts; image hygiene; incident cases in Dashboard.	Outweighs (analytics value > residual medium impact).
Stream processing & alerting	Clear audit of steps	Runtime compromise traces	P2-R11	Forensics needs step-wise lineage.	LOMOS transformation lineage & hashes; IR playbooks in Dashboard.	Outweighs strongly (audit materially lowers impact).
Backend patient-data DB & access	Longitudinal timeline	Key compromise → bulk decrypt	P2-R12	Timeline value increases impact of key loss.	FE4MED (KIA) lifecycle & rotation; LOMOS key-use audit; least-privilege services.	Outweighs (clinical value high; residual low with KIA).
Stream processing & alerting	Fault tolerance	Covert egress from service	P2-R13	Surviving faults means catching quiet exfil channels.	LADS beacon/egress modelling; LOMOS timeline correlation; containment in Dashboard.	Outweighs (resilience gain significant; residual medium).

Table 6 Sample of the benefit risk analysis performed on pilot 2

The resulting analysis was introduced in the risk management tool (please refer to Figure 9, Figure 10, Figure 11 and Figure 12).

Funded by Horizon Europe Framework Programme of the European Union

Figure 10: Risk Management Tool showing the risk analyses Dashboard for Pilot 2

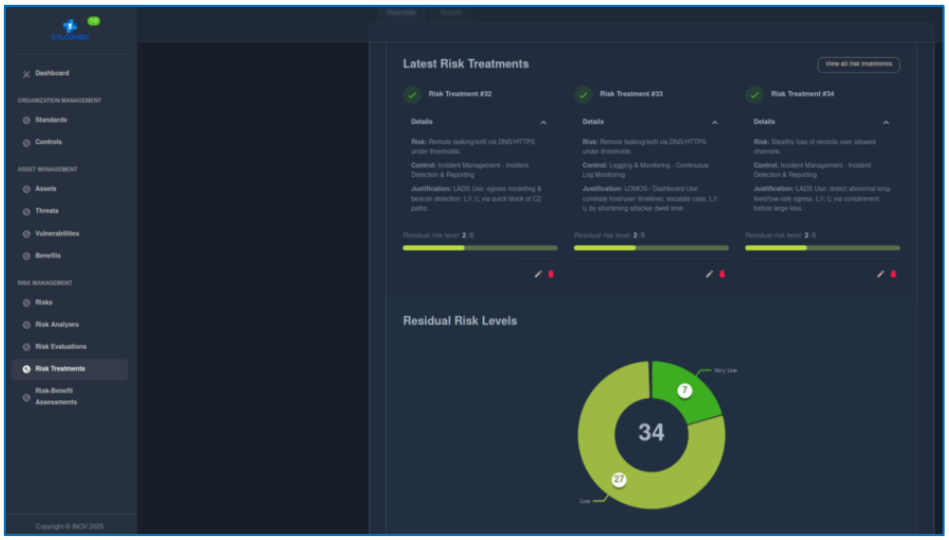

Figure 11: Risk Management Tool showing the Dashboard with the risk treatments results on risk levels for Pilot 2

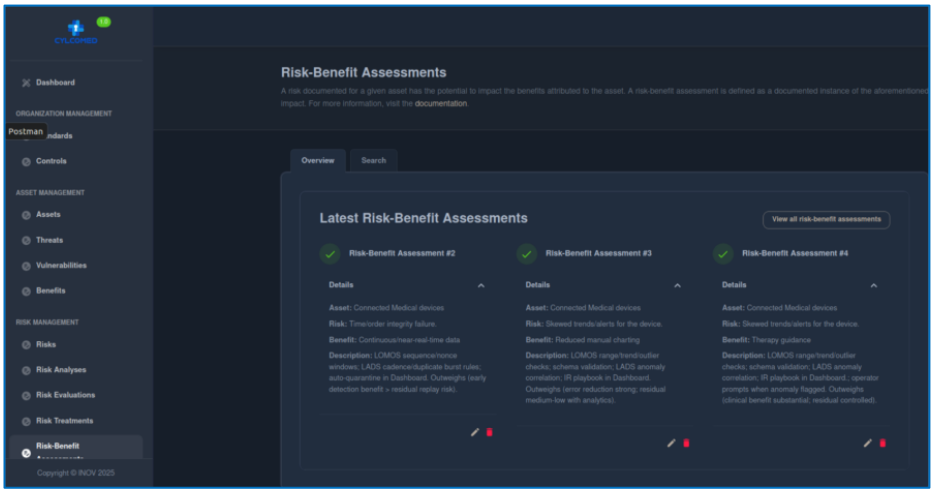

Figure 12: Risk Management Tool showing the Dashboard with the benefit-risk assessment for Pilot 2

Funded by Horizon Europe Framework Programme of the European Union

3 Task 6.3: Validation of the pilots

This task focuses on validating the CYLCOMED system in the two project pilots. In both Pilots, the validation process is conducted following two complementary approaches: a technical evaluation and a cross-functional (non-technical) evaluation.

The approach applied differs for each component: in the technical validation, the technical partner evaluates a specific set of metrics to assess whether the system meets the defined requirements. While the non-technical validation process involves interviewing key stakeholders in the hospital where the pilot studies are conducted, or the clients when technical work has been tested under laboratory conditions

3.1 Validation of the system in Pilot 1

3.1.1 Technical Validation of Pilot 1

We have incorporated CYLCOMED Cybersecurity tools in the medical system, and we have verified that the performance of the system is not altered by the incorporation of this new cybersecurity SW components. First, we have captured the real time results about the system´s behaviour in the digital twin –test bench- under laboratory conditions obtained under simulated conditions and in second place we have compared these results with those obtained with the medical system incorporating the cybersecurity tools.

The results have proved to be identical in both cases, particularly when testing the controller under real time conditions.

Here are the results obtained (there is also a video presentation available upon demand):

Encryption / Decryption (FE4MED tool)

The following images show how data is sent to the server from the Raspberry PI (RPI). We start with a database, which is empty in order to visualize things more easily.

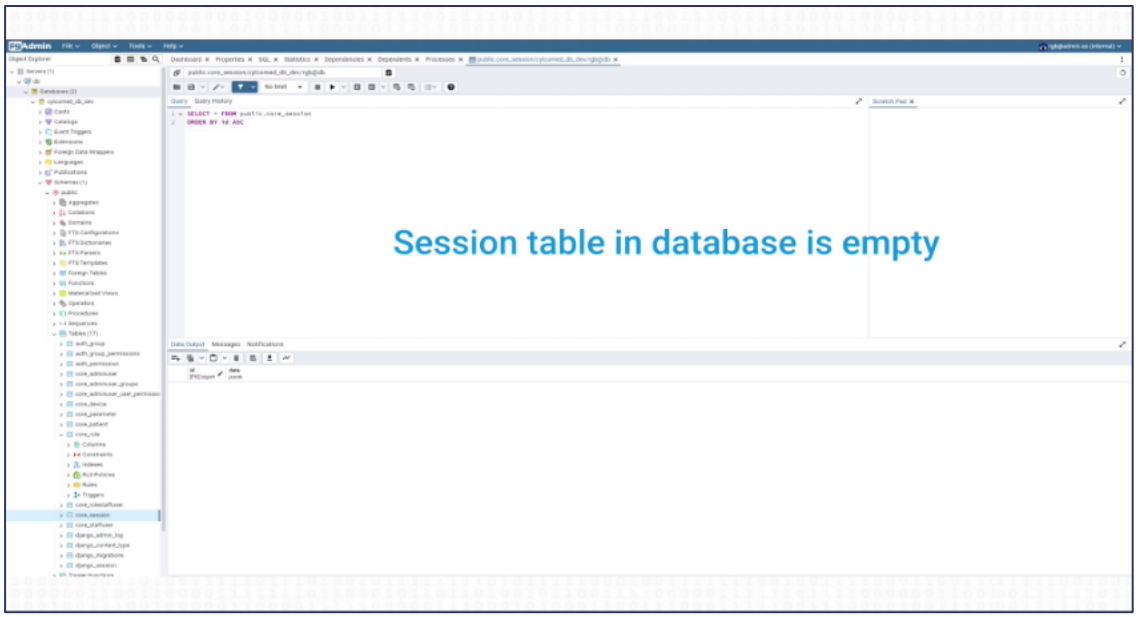

Figure 13: Start of encrypted data transmission session (FE4MED): This figure shows the initiation of a secure communication session between VisionAir and the Raspberry Pi, followed by the creation of a unique session identifier (ID 273) in the server database. All subsequent transmissions in the pilot use this identifier to ensure traceability and secure linkage of encrypted physiological data.

Funded by Horizon Europe Framework Programme of the European Union

At start, a session between Vision Air and the RPI was created. Then, after a new session was created between the RPI and the server, a new entry with a unique session identification number was created in the server database (identifier 273). Since then, this identifier number has been used in all transmissions.

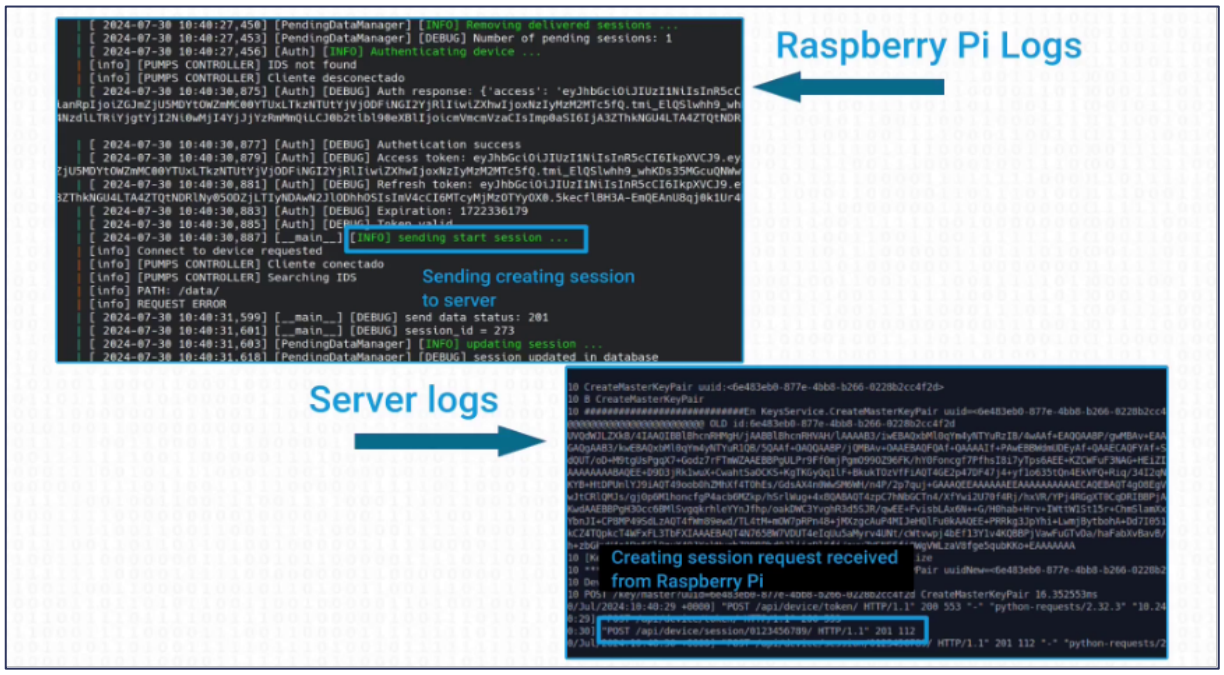

Figure 14 Encrypted data storage process in the server (FE4MED). This figure illustrates the flow of encrypted physiological parameters sent from the Raspberry Pi through the FE4MED tool and stored on the server under session ID 273. The system returns a confirmation code after successful encrypted data insertion.

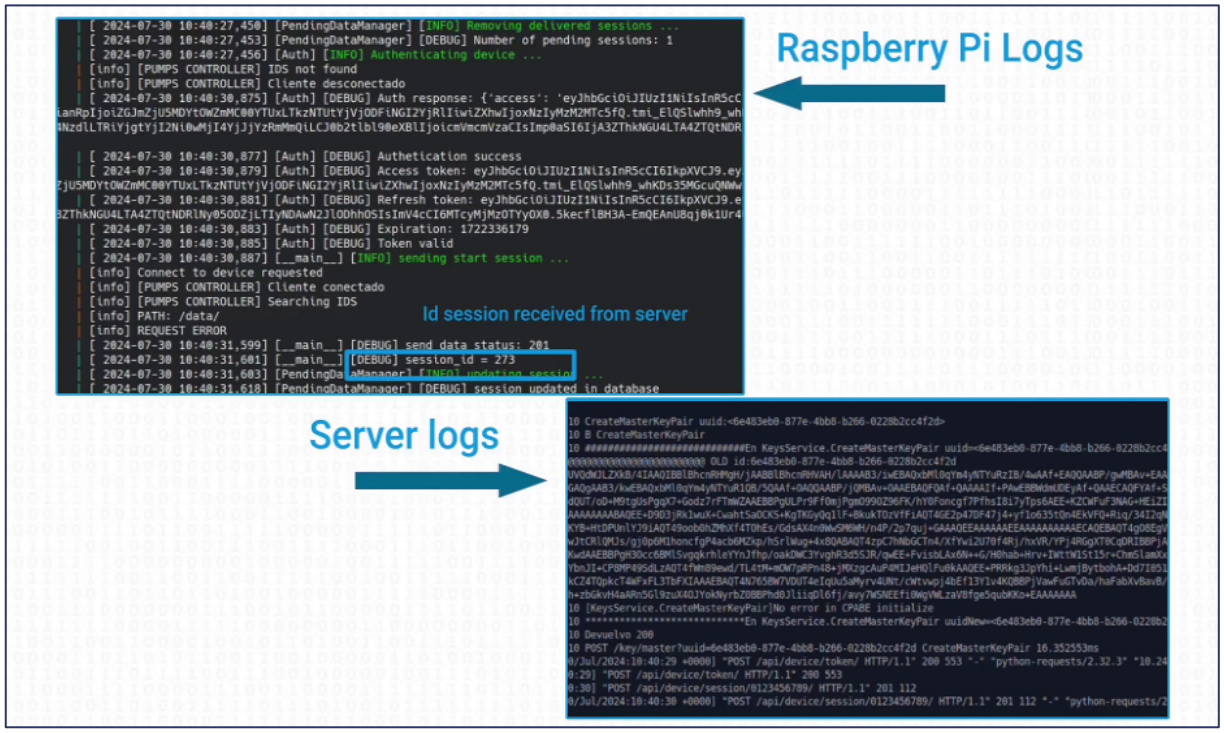

Figure 15 Log records of FE4MED encrypted database queries. This figure presents log messages generated during requests made to the encrypted database. It demonstrates the proper retrieval of encrypted entries before decryption and verification.

Funded by Horizon Europe Framework Programme of the European Union

Data received by the RPI from the Vision Air is sent through the EVIDEN tool FE4MED in order to encrypt each physiological parameter with its corresponding policy and then it is sent to the server via 273 identification session number. Therefore, this is the way through which the data is stored in the database, and when we do that, we return a code, indicating that everything was OK.

The logs show the requested data from the encrypted database.

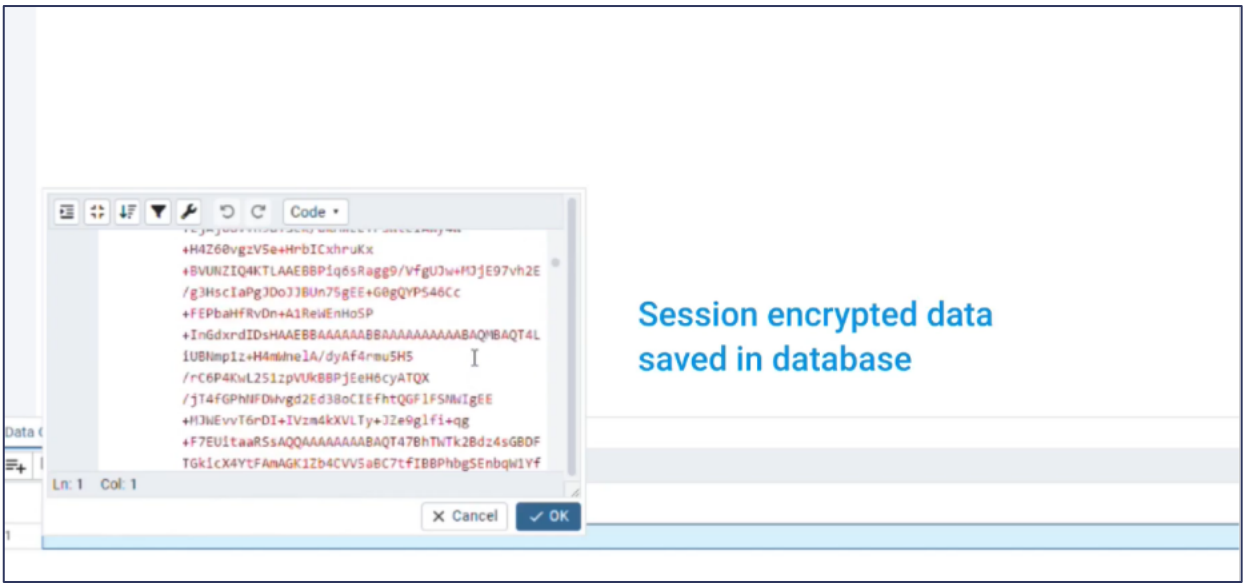

Figure 16 Encrypted data stored in the database. This figure displays how physiological data is stored in encrypted form in the server database. It supports verification that received data is correctly encrypted end-to-end.

If we now go to the database, we can see that the data has been properly received in an encrypted way and we can visualize it afterwards by accessing this encrypted information.

Then we use the EVIDEN tool FE4MED to decrypt this information and then the decrypted data can be compared to the original one, and we can make sure that everything fits.

The process consisted in asking for data with identifier 273 which returns as a JSON document with data that is already decrypted and then comparing this data with the original ones.

Funded by Horizon Europe Framework Programme of the European Union

Figure 17 Decryption and validation of original vs. decrypted data. This figure shows decrypted physiological parameters returned as a JSON document using the FE4MED tool. A comparison with the original data confirms the accuracy and integrity of the decryption process.

When a user of the medical web platform wants to access to the patient data, she only will be able see the parameters that her role attributes provide.

In the case of users who have role “doctor1” with attributes “t1”, “t2”, “hr”, and “SpO2”, they will see these parameters but not NMT measures as can be seen in the figure below.

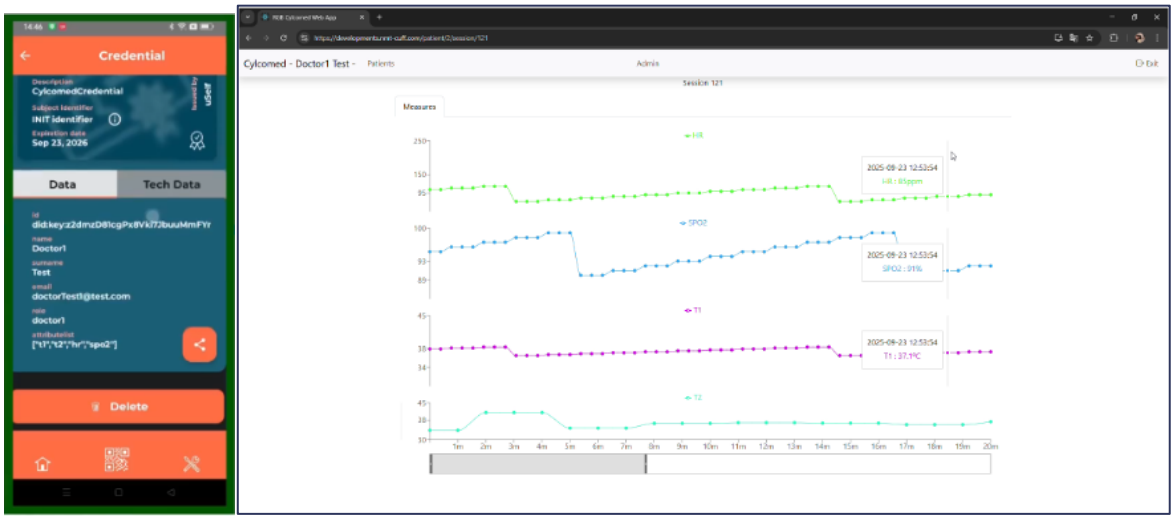

Figure 18 Data visualisation for user with role “doctor1”. This figure demonstrates role-based access to patient parameters. Users with the “doctor1” role can view parameters such as t1, t2, HR, and SpO_2, but cannot access NMT metrics.

In the case of users who have role “doctor2” with the same attributes as role “doctor1” but “nmt” attribute too, they will see NMT values too.

Funded by Horizon Europe Framework Programme of the European Union

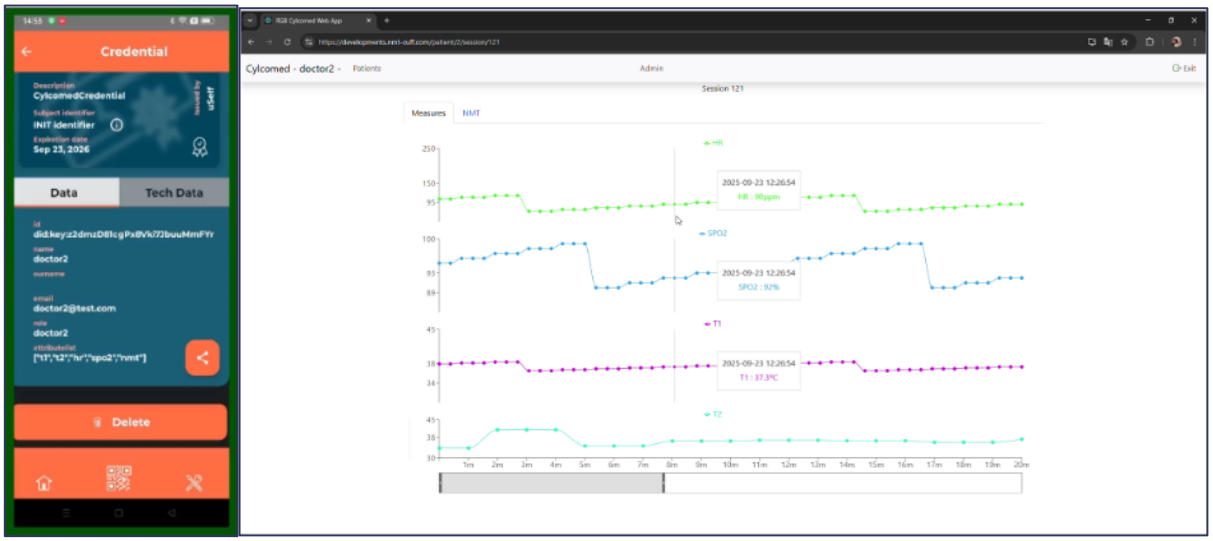

Figure 19 Data visualisation for user with role "doctor2" including NMT data. This figure illustrates extended access rights. Users with the "doctor2" role—who have all "doctor1" attributes plus NMT—can view neuromuscular transmission values in addition to standard parameters.

Figure 20 Additional example of role-based data access. This figure provides another representation of differentiated access to patient data, highlighting consistency in the authorization model implemented via C-OPA and FE4MED.

Authentication (LuS4MED tool)

This app is used to generate user credentials and give then access to the web platform where the patient data is stored. The first step to access the web platform is to issue credentials for the previous registered users in the web platform who has their assigned roles.

When user enters their mail in the registration web LuS4MED app generates a QR code that should be scanned by UsefApp installed in a Smartphone. Fingerprint will be required in order to access the application.

Funded by Horizon Europe Framework Programme of the European Union

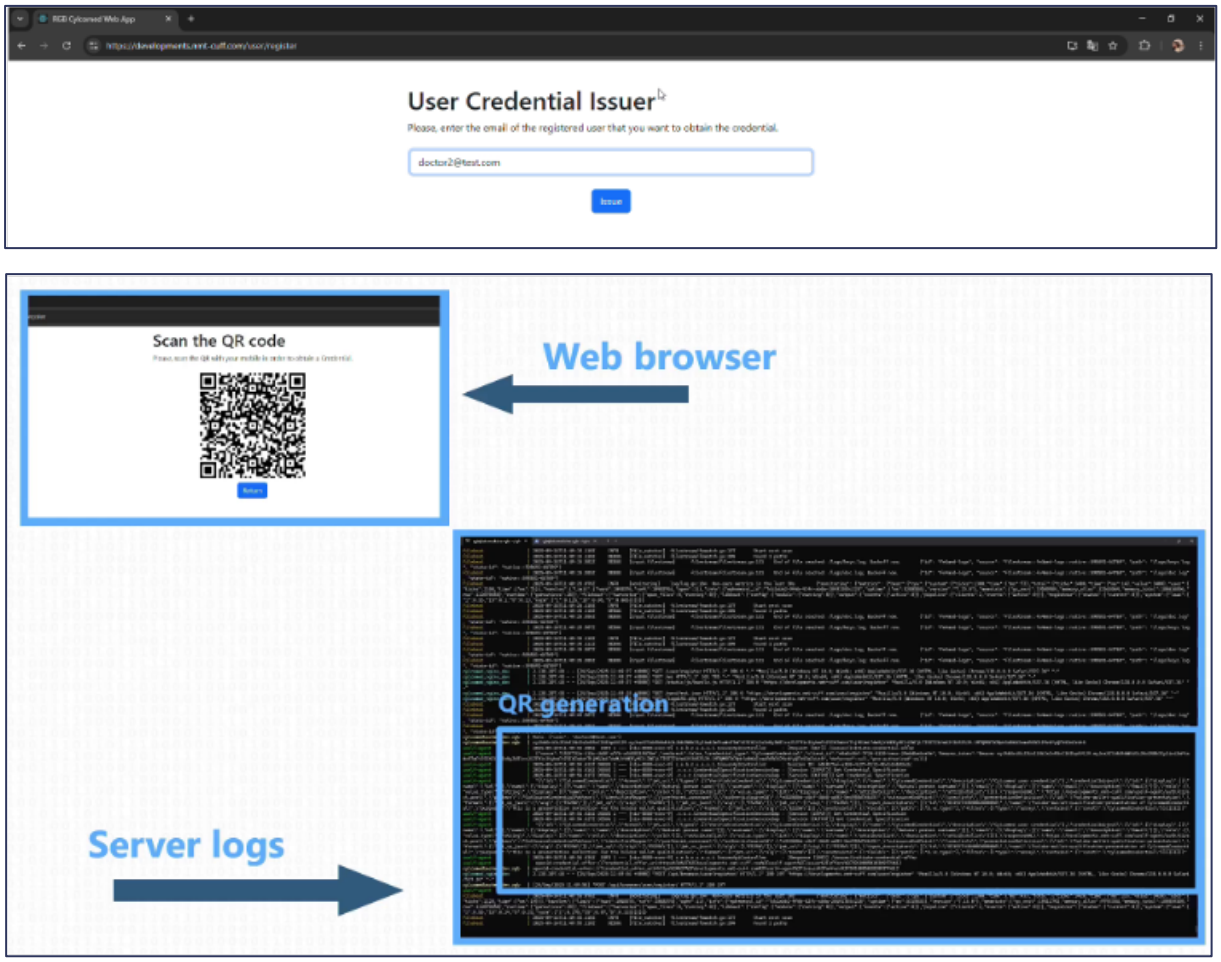

Figure 21 Credential generation using LuS4MED This figure shows the initial step of the credential issuance process: entry of the user's email into the registration interface, triggering the generation of a QR code to be scanned by the UsefApp mobile application.

Once the QR code is scanned by a user then should select a name and accept the credential, and the credential will be stored into the app.

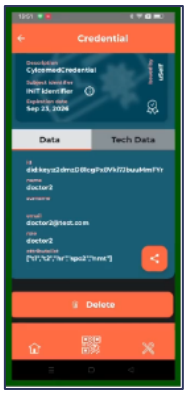

Figure 22 Credential acceptance in the UsefApp mobile application. This figure depicts the interface by which a user scans the QR code, selects a username, and accepts the digital credential, which is then stored in the mobile application.

The logging process involves entering the main page of the web platform and scanning the QR code generated by the LuS4MED application. When the QR code is scanned, the user

Funded by Horizon Europe Framework Programme of the European Union

must provide credentials and accept. After this, the access token is obtained, and the user can navigate the platform.

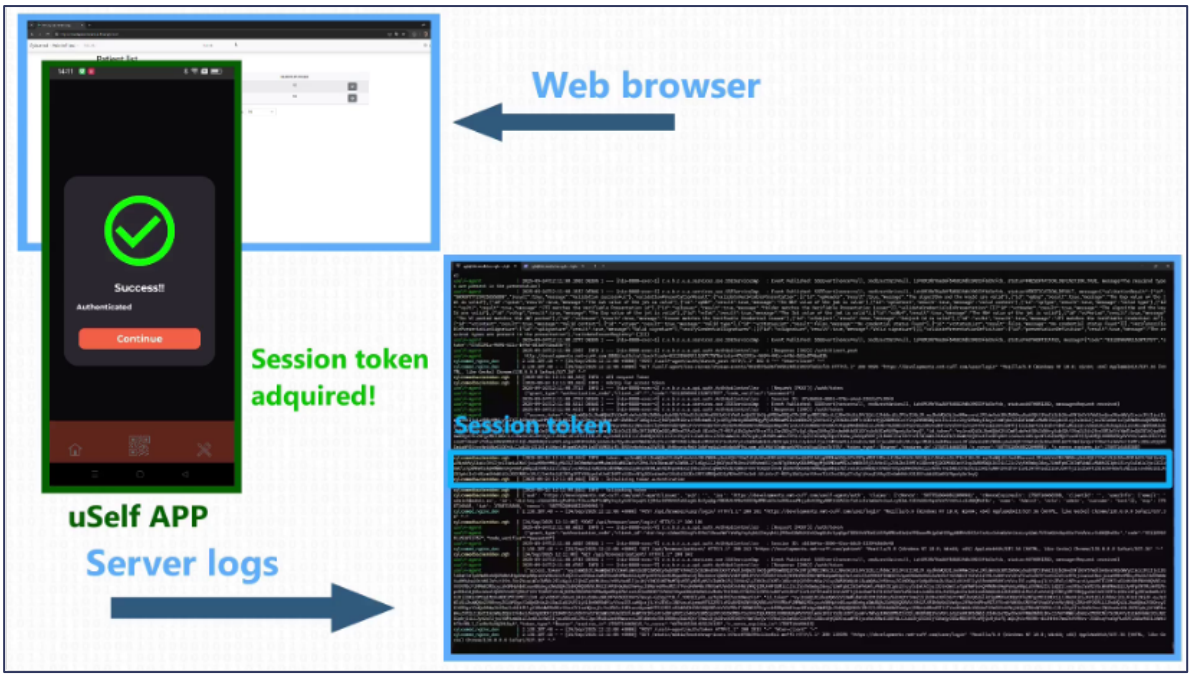

Figure 23 Login workflow using QR-based authentication. This figure presents the LuS4MED login process: scanning the QR code on the web platform, submitting credentials, and obtaining an access token to navigate the platform securely.

Authorisation (C-OPA tool)

This tool works as a proxy between user and FE4MED service and allows or denies access to patient data or policy management depending on the user's role. When users have the correct role, they cannot access patient data as seen previously.

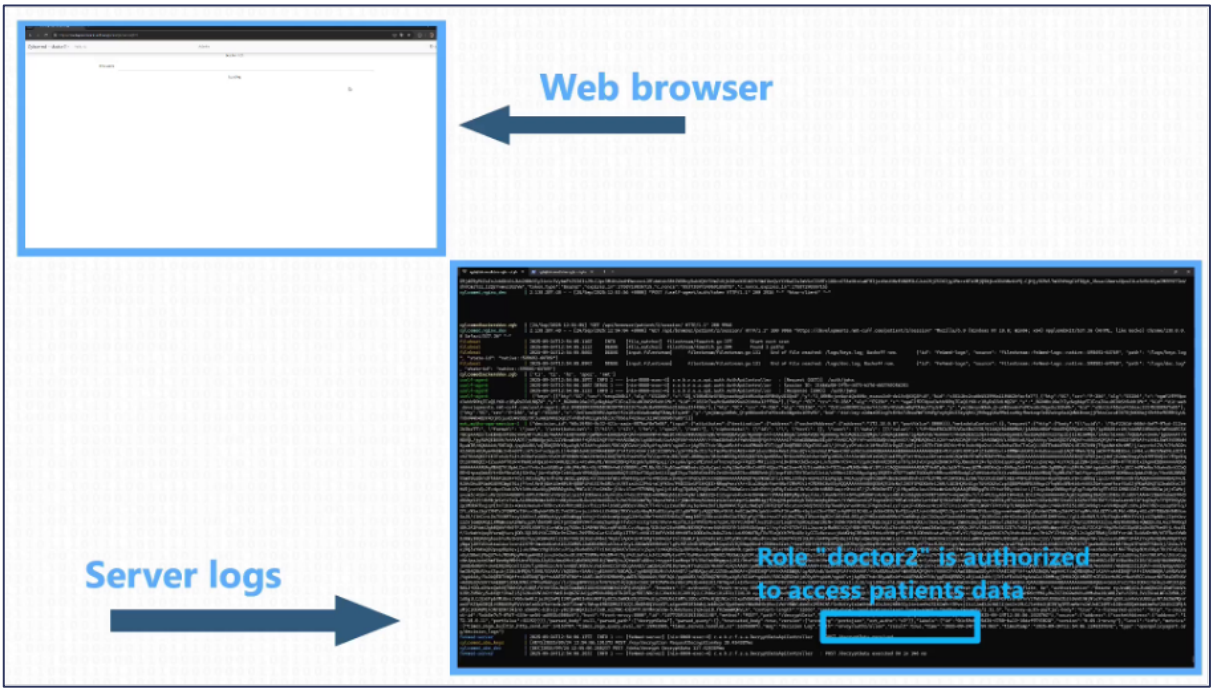

Figure 24 Authorized access to patient data (C-OPA). This figure shows how the C-OPA authorization layer allows or denies access to patient data depending on the user's assigned role and permissions.

Funded by Horizon Europe Framework Programme of the European Union

But if a user with “admin” role tries it, the access is denied.

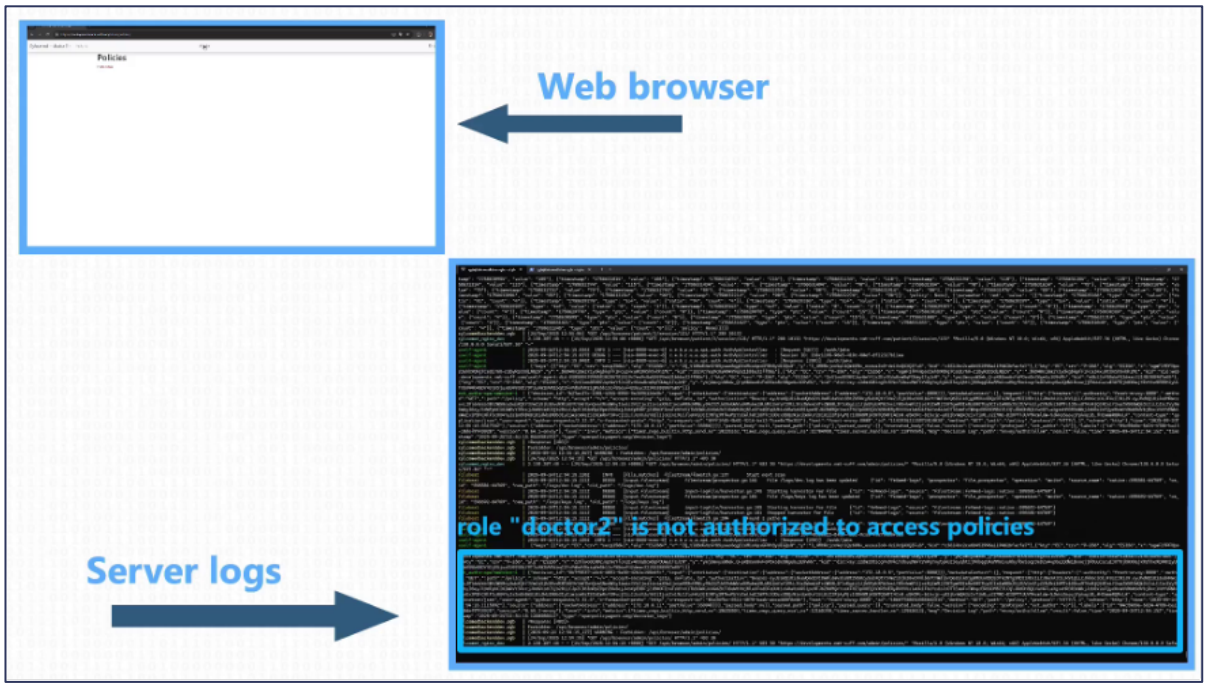

Figure 25 Access denial for “admin” role attempting to retrieve patient data. This figure illustrates a scenario where a user with an “admin” role is denied access when attempting to view patient data, demonstrating policy enforcement.

If a user with a role different from “admin” tries to access policy management, access is denied too.

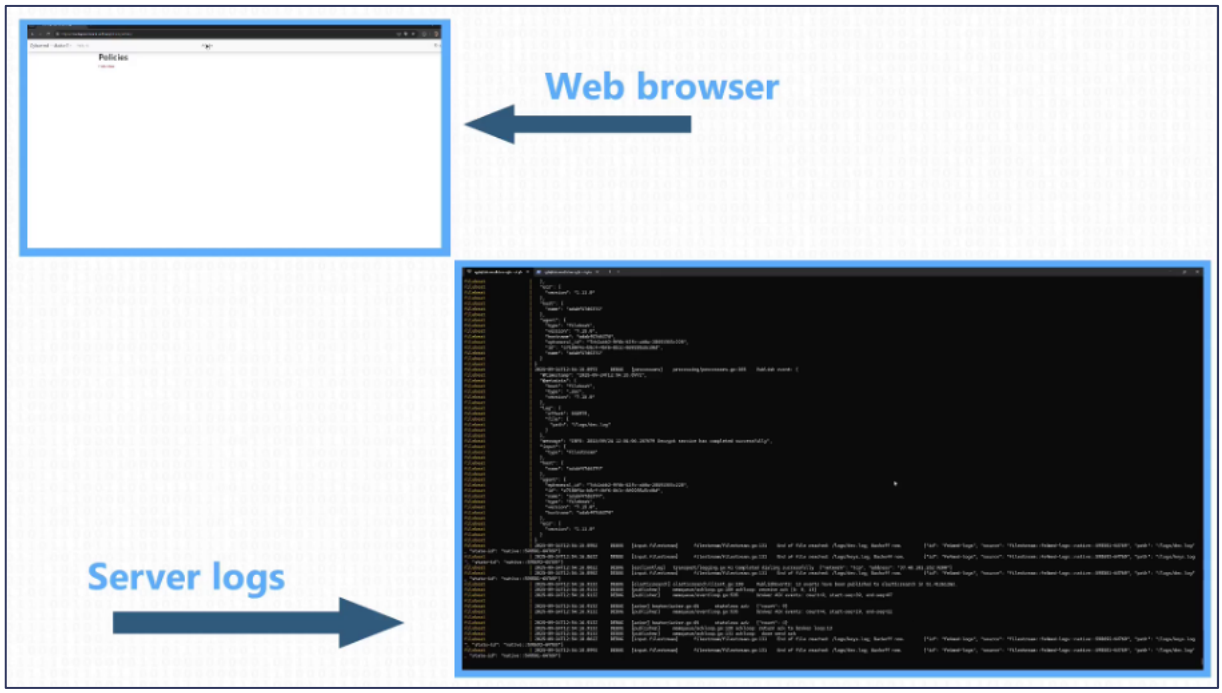

Figure 26 Denied access to policy management for unauthorized users. This figure shows how users without the “admin” role are prevented from accessing policy-management functions, reinforcing role-based restrictions within the C-OPA tool.

Network Vigilance (LADS)

Funded by Horizon Europe Framework Programme of the European Union

For Pilot 1, the CYLCOMED Security Dashboard and the LADS "brain" were deployed on an ATOS/EVIDEN server. To detect suspicious behaviour in the network, LADS's telemetry sensors have been installed in the RGB's web platform server, in the RasPi, and in the Atos's server where the LADS brain and other CYLCOMED tools of the toolbox were deployed. In this setup, all important endpoints of the pilot were monitored by the LADS.

In RGB's laboratory, LADS sensors captured network traffic and forwarded flow telemetry over secure network channels to the ATOS/EVIDEN instance, where it was processed and visualised in the Dashboard. This hybrid setup allowed us to keep probing and analytics off the lab network while maintaining encrypted, controlled data paths end-to-end.

Dataset and labelling.

We configured LADS to train for 6 hours on all traffic across the three endpoints and then performed validation (monitoring) on all traffic of the endpoints for 15 hours.

Across the evaluation window we processed 1090125 flows. LADS flagged 247031 as anomalous and 843094 as normal. To approximate ground truth, public IPs observed in all flows were cross-checked against CTI sources *abuseipdb.com* and *virustotal.com*, yielding a "***Malicious IP***" reference set of ***9248*** IPs (out of 12346 total CTI entries).

Results Confusion Matrix

Table 7 and 8 shows the confusion matrix of the evaluation results.

	Predicted Positive	**Predicted Negative**
Actual Positive (CTI-positive)	217527 (TP)	0 (FN)
Actual Negative (CTI-negative)	29504 (FP)	839580 (TN)

Table 7: Confusion Matrix - LADS Pilot 1

Metric	**Formula**	**Result**
Accuracy	(TP + TN) / (TP + TN + FP + FN)	97,28%
Precision (PPV)	TP / (TP + FP)	88,06%
Recall (Sensitivity)	TP / (TP + FN)	100%
F1-score	2·(Prec·Rec) / (Prec + Rec)	93,65%

Table 8: Shows the metrics calculated based on the confusion matrix

Results Malicious Activities Detection

Funded by Horizon Europe Framework Programme of the European Union

The analysis of the network flows captured in the RGB pilot shows a significant presence of malicious external IP activity. Using AbuseIPDB and VirusTotal as reference intelligence sources, we identified that a large portion of the malicious traffic originated from Brazil and the United States (Figure 27)

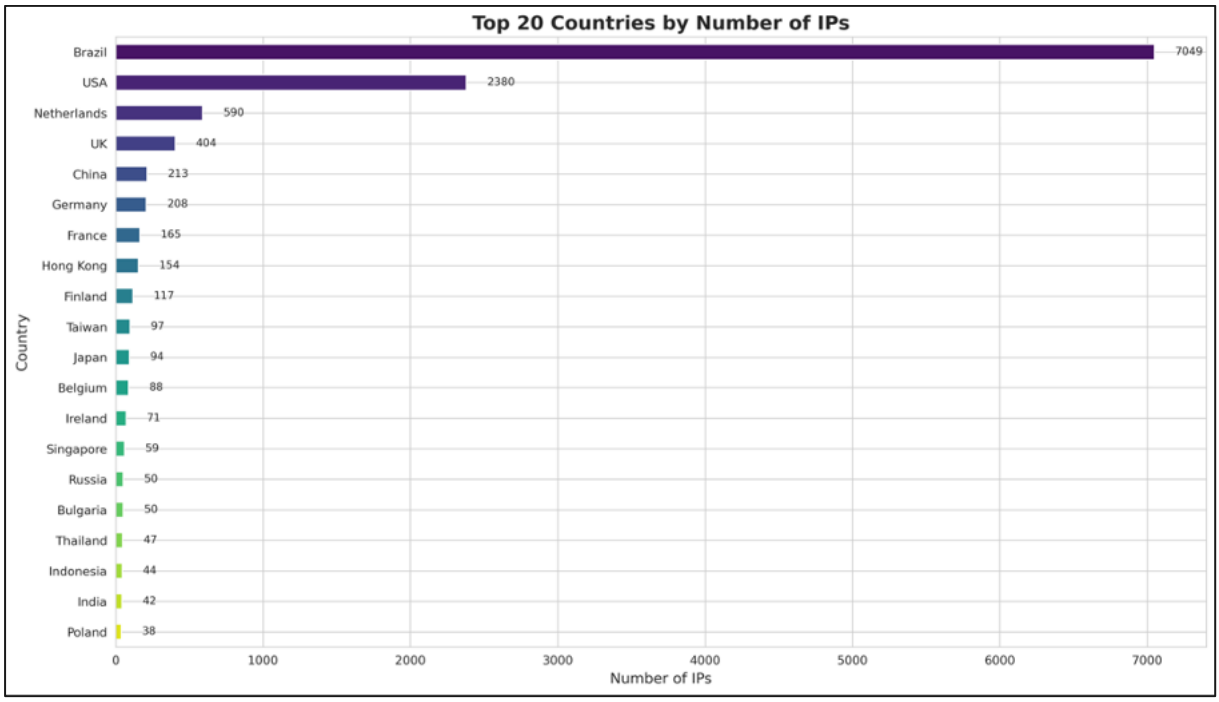

Figure 27: Top 20 Countries

Regarding the overall distribution, approximately two-thirds of all identified IPs presented evidence of malicious activity, while the remaining third corresponded to clean or previously unreported traffic (Figure 28)

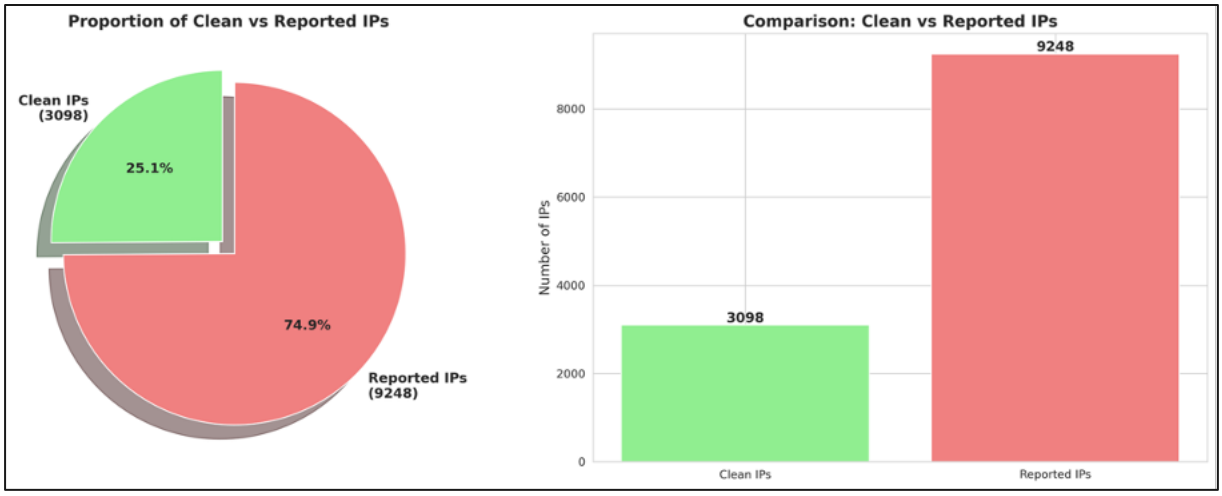

Figure 28: Reported vs Not Reported Ips - RGB

In terms of attack typology, the most frequently observed categories were DDoS, Brute Force, and Port Scanning, indicating an active pattern of reconnaissance and credential-stuffing attempts against the monitored systems (*Figure 29*). These trends are consistent with automated campaigns that scan for Internet-exposed vulnerabilities.

Funded by Horizon Europe Framework Programme of the European Union

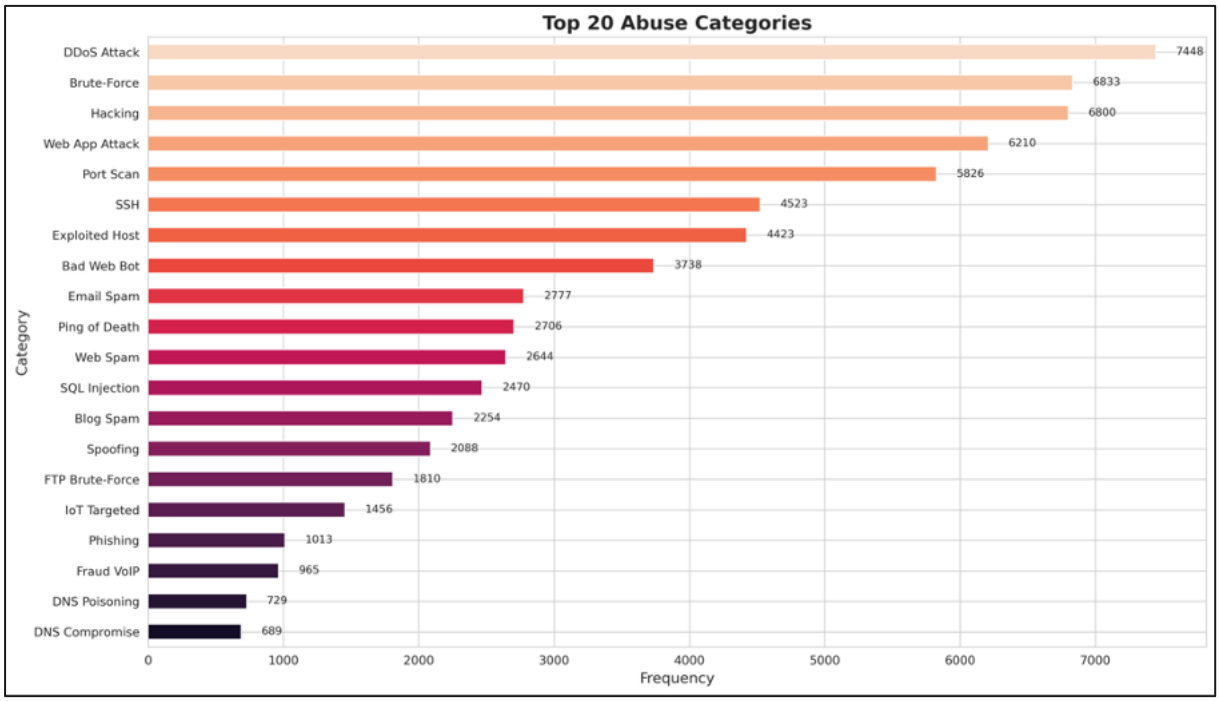

Figure 29: Reported Category Attacks - RGB

The most representative, aggressive, communications were from Brazil (Sao Paulo) from IP address range of 131.100.70.xxx–131.100.75.xxx representing *SYN-flood-like* behaviour, *unauthorised access* attempts, as well as *too many connections abuse*.

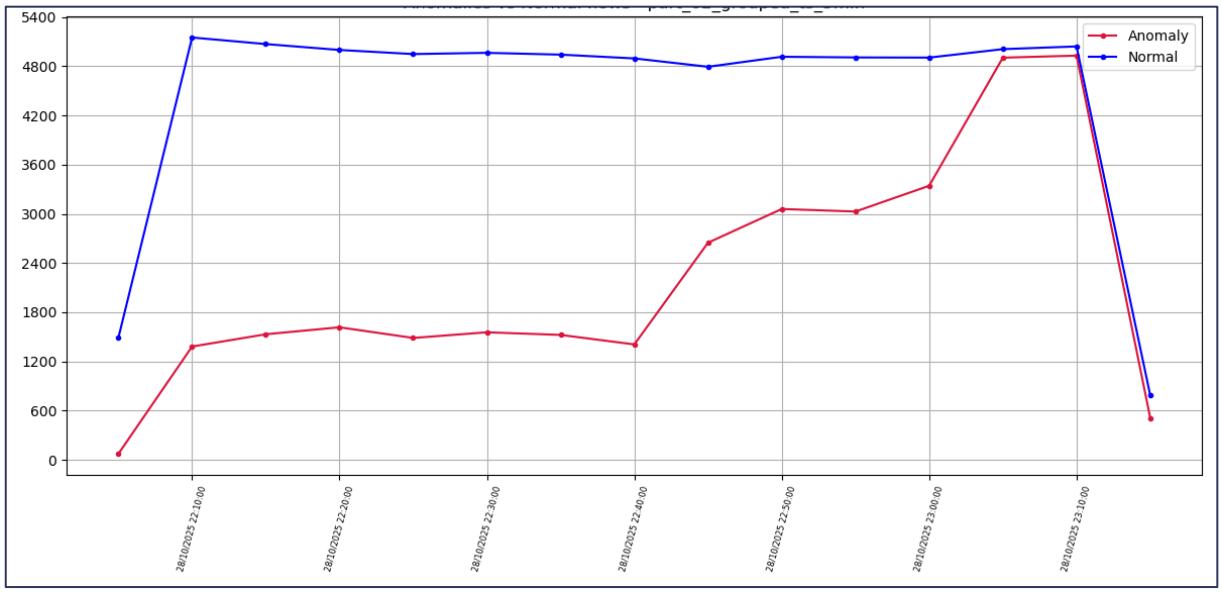

Figure 30: Pilot 1 RGB Malicious Activities Detection Sample by LADS

Figure 30 shows the number of normal flows versus anomalous flows for the period of 28/10/2025 22:50–23:10h UTC, as displayed on LADS's Dashboard. We observe that the volume of malicious (anomalous) traffic, in this case the number of flows, did not exceed the normal flow volume (blue line), but still represented a high number of malicious attempts compared to the normal baseline traffic. Almost all malicious attempts during this period targeted the IP addresses of the RGB server.

System Behaviour (LOMOS)

The logs generated by FE4MED application in the RPi and in the server are sent to LOMOS server.

Funded by Horizon Europe Framework Programme of the European Union

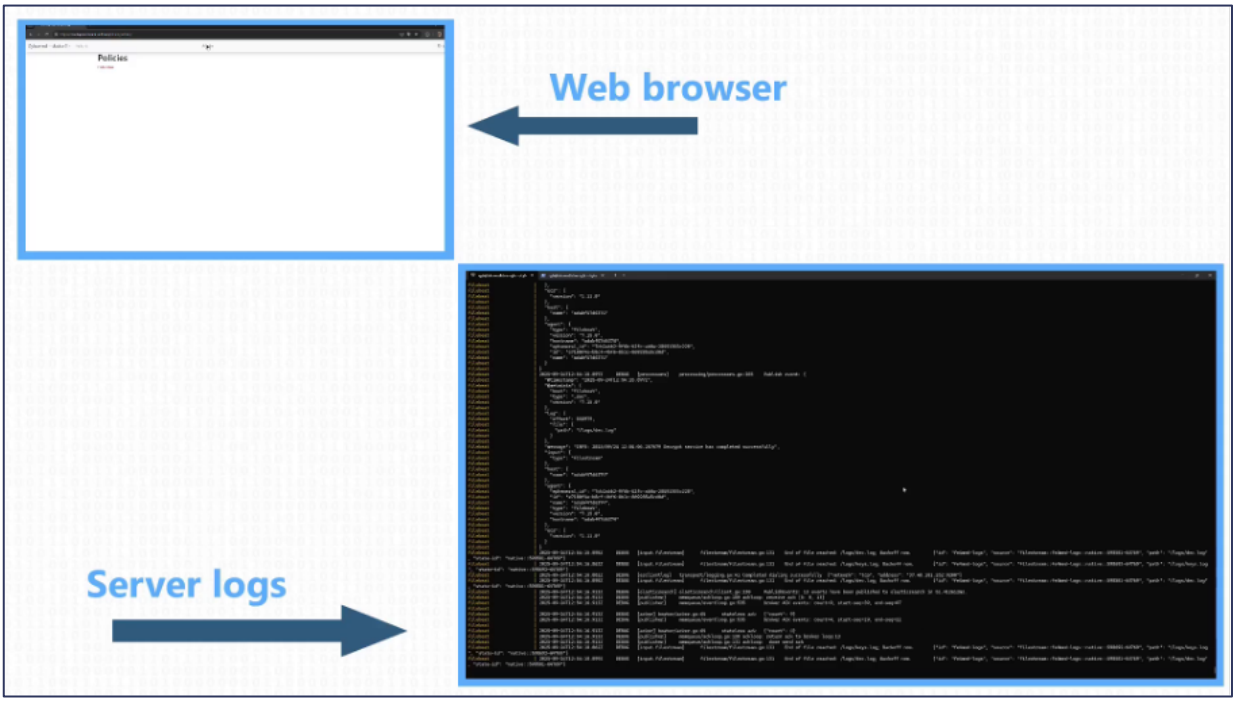

Figure 31 System logs sent to the LOMOS monitoring server. This figure illustrates how system behaviour is captured through the logs generated by the FE4MED application, both on the Raspberry Pi and on the central server. These logs are transmitted to the LOMOS platform, which performs continuous monitoring and detection of anomalies in the system's operation.

In parallel with this one, we have the medical system set and running, so that we replicate the medical functionality now with the cybersecurity tests in place. This is what we get:

PATIENT SIMULATOR TEST CASES

The testing procedure has been performed in two steps: first, the results described have been obtained without using Cybersecurity tools. Secondly, cybersecurity tools (as described in D5.3) have been incorporated, yielding the same results.

We have succeeded in implementing the medical functional functionalities and integrated all pieces of CYLCOMED cybersecurity tools in the Testbench platform. The cybersecurity tools do not require much CPU, and we have concluded that cybersecurity tools do not alter the normal behaviour of the medical system.

In this regard, the testbench platform tool has been successfully tested and shows its validity in the definition of the performance of the control algorithm, under SW cybersecurity performance. A substantial number of test cases have been performed to prove its validity, first in the patient´s model behavior and then the control algorithm. For this purpose, the control algorithm developed by RGB has been tested. The objectives of CYLCOMED in the development of this tool have been fully achieved.

PATIENT SIMULATIONS

In order to verify the correct behavior of the simulator, the simulator has been run with different patient configurations. In these tests, an initial dose of relaxant has been applied to the simulated patient, and the control has been allowed to evolve (without applying additional doses) until complete recovery.

The tests carried out allow to verify the controller performance under different patient conditions such as:

Funded by Horizon Europe Framework Programme of the European Union

Volume of Distribution (Vd) : When the drug is injected into the patient, it is dispersed in a volume known as the “volume of distribution” and is expressed in ml/kg.

Cp50: is the plasma concentration which would, at a steady state, produce 50% depression of NMT response. This means that the lower the Cp50, the more sensitive the patient is to the drug.

Initial Dose: The control performance depends on the initial drug doses, at the beginning of the operation. The higher the dose, the higher the concentration in plasma, and therefore the longer the drug remains in the patient, prolonging his recovery.

NMT CONTROL PERFORMANCE

Once the correct operation of the patient simulator has been verified, we apply a control algorithm to evaluate RGB´s NMT control strategy. The control algorithm is based on Fuzzy Logic technology.

In order to assess the effectiveness of the strategy, several controls are performed by varying the patient's parameters of Vd and Cp50. The following graphs show the results obtained.

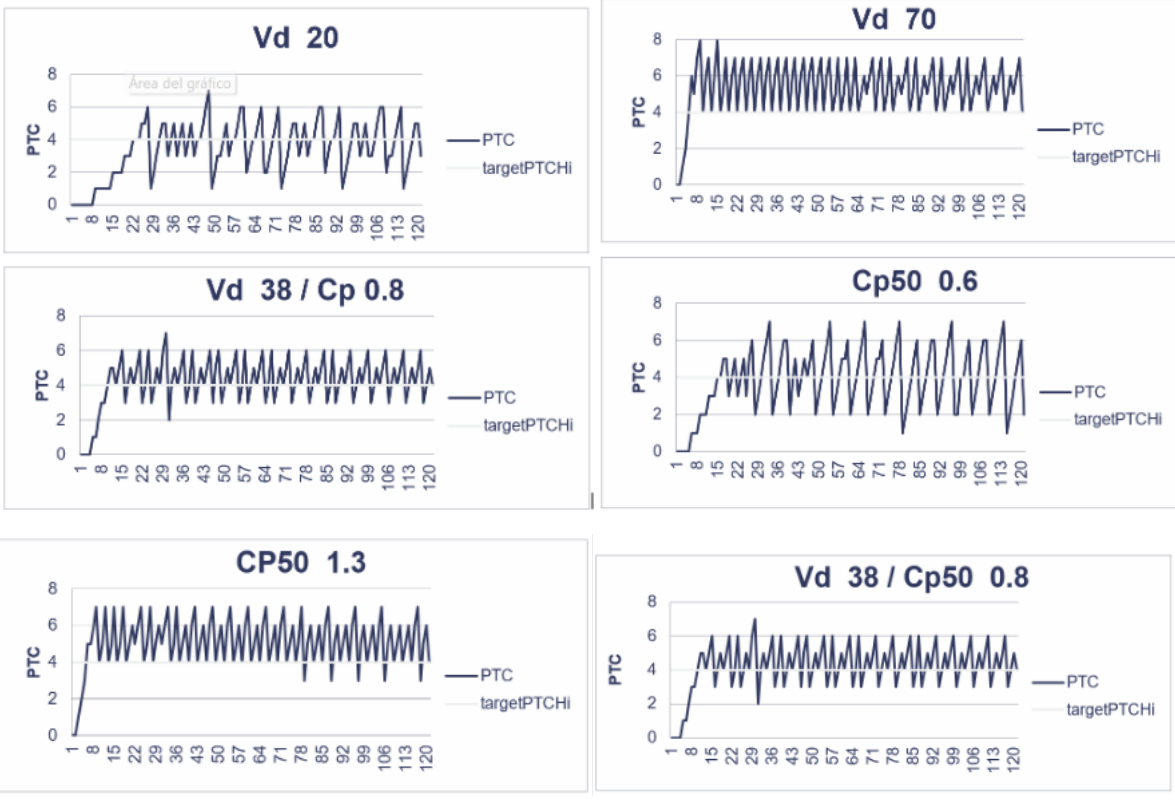

Figure 32: Results obtained from varying patient's parameters of Vd and Cp50

METRICS OF THE VALIDATION PROCESS OF THE INFUSION CONTROLLER PERFORMANCE

Funded by Horizon Europe Framework Programme of the European Union

	Target PTC	*Media PTC*	*(sd)*	*PTC Above (%)*	*PTC Below (%)*	*PTC Target (%)*
Vd = 20 ml/kg	4	3.94	1.4	31	48	21
Vd = 38 ml/kg (*)	4	4.5	1.05	45	25	30
Vd = 70 ml/kg	4	5.53	1.46	71	3	26
Cp50 = 0.6 µg/mL	4	4.22	1.56	41	42	17
Cp50 = 0.8 µg/mL (*)	4	4.5	1.05	45	25	30
Cp50 = 1.3 µg/mL	4	5.25	1.15	67	8	25

Table 9: Control data applied to a specific target

(*) Are the same control.

Control strategy is best achieved when the patient's configuration matches standard values (Vd = 38 mL/kg, Cp50 = 0.8 µg/mL). In this case, the standard deviation is the lowest (1.05) and the time spent on target is also the highest (30%).

When the patient's configuration is not very sensitive to the drug (high Vd or high Cp50), then the dose applied by this strategy is insufficient and the NMT value remains above the target for a long time (71% and 67%).

When the patient's configuration is very sensitive to the drug (low Cp50), then the dose applied by this strategy causes large variations in the NMT value (its standard deviation is very large 1.56)

METRICS OF THE VALIDATION PROCESS OF THE CYLCOMED CYBERSECURY TOOLS PERFORMANCE

The table below show the conclusions of performance of all CYLCOMED tools. The table includes the following details: Integration in the system; Overhead: the average time increase in operation compared with the baseline system without cybersecurity tools; Verified performance compared to baseline: how the integration of the tool affects the system comparing with the baseline.

CYLCOMED tool	**Integrated (Y/N)**	**Overhead**	**Verified performance compared to baseline**
FE4MED (enc)	Y	12ms	Does not affect system performance
FE4MED (dec)	Y	347ms	Does not affect system performance
LuS4MED	Y	Not applicable	The security benefits outweigh any potential login delays on the platform
C-OPA	Y	158ms	Does not affect system performance
LOMOS	Y	51ms	Does not affect system performance

Funded by Horizon Europe Framework Programme of the European Union

LADS	Y	Not applicable	Does not affect system performance

Table 10: CYLCOMED tools performance conclusions

		OVERHEAD				
Component	**Integrated (Y/N)**	**Number of measures**	**Mean value**	**Number of measures**	**Mean value**	**Verified performance compared to baseline**
FE4MED	**Y**					
Encrypting JSON (s)		11	2.6154 *	802	3.4085 **	Does not affect performance
Decrypting JSON (s)		3	42.3936 *	144	161.2222 **	Does not affect performance
Decipher Key Generation (ms)		3	4.1725	144	5.146	Does not affect performance
Key Pair Generation (ms)		1	2.855	1	106.786	
LuS4MED	**Y**					
Issuing VC (s)		N/A	N/A	1	3.8762	Does not affect performance
Present VC (s)		N/A	N/A	84	0.1289	
C-OPA (ms)	**Y**	N/A	N/A	N/A	158	Does not affect performance
LOMOS (ms)	**Y**	N/A	N/A	N/A	51	Does not affect performance
LADS	**Y**	N/A	N/A	N/A	N/A	Does not affect performance
(*)1 parameter encrypted. (**) 4 parameters encrypted. N/A Not available data.						

Table 11: Overhead measurements for CYLCOMED components.

For **FE4MED** component, initial measures for encrypting, decrypting and key generation (master key pair and decipher key) were taken before the integration phase. As indicated in the table, the number of measures were very low, and small JSON data were encrypted (only one parameter encrypted), but significant enough at this early stage for establish a base line. Once the FE4MED was integrated, additional measures were taken considering the whole process. In this integration stage, a high number of measures were available and the size of the JSON data to be encrypted was bigger (4 parameters were encrypted). This implies that the time for both, encryption and decryption was increased. In the case of decryption process, the time is four times bigger but is necessary to consider that the decryption process implies to check if the ciphered parameter policy maps with the decipher key's attributes, which means that as more encrypted parameters more time to check and decipher. Regarding the key generation, additional measures must be taken for this purpose, namely the master key pair generation, but considering that this is made only once when the system is launched, the impact on the general process is not significant.

In the case of **LuS4MED** component only measures were taken during the integration process. Although the process for issuing a VC is less than 4 seconds (more measures need to be

Funded by Horizon Europe Framework Programme of the European Union

taken), this process is performed by the user only once, which means that the impact on the general process is quite low. The important aspect is that the validation of the present proof sent by the user for accessing the system is quite low.

3.1.2 Non-Technical Validation of Pilot 1

As RGB is operating in the anaesthesia market, with the sales of certified VISION DUO and VISION Air monitors, we have access to anaesthesiologists as well as medical equipment distributors that already know well the benefits of the infusion controller, the integration problems in the Operating Room, recovery room or ICU, and the potential market for the product.

The feedback we have obtained is unanimous regarding the need of this type of equipment, even more considering the trend towards robotic operations. The cybersecurity concerns are well known, although it is assumed by medical stakeholder that this is outside their scope, and therefore need certified and proved solutions. Anaesthesiologists showed a particular interest on having good identification solutions, and the need that these are ergonomic and quick. The particular conditions in which they operate represent a big challenge, since the anaesthesiologist has no time to devote to identification when the condition of the patient is severe and, on the other side, the risk of device misuse is very critical (hazards due to e.g. an unauthorized user getting access to the device), even though the access to the wards are highly restricted.

3.2 Validation of the system in Pilot 2

3.2.1 Technical Validation of Pilot 2

Based on the structured validation checklist (see Protocol v1.0), the following dimensions were tested:

Technical Validation criteria	
System Functionality	Simulation-based feature validation Ensuring the telemonitoring system and cybersecurity tools perform according to design specifications.
Integration	Verifying seamless integration with hospital IT infrastructure and workflows
Reliability and Performance	Assessing stability, uptime, response times, and resilience under various conditions
Interoperability	Confirming compatibility with existing hospital systems, medical devices, and communication protocols.
Safety Compliance/Risk management	Ensuring adherence to clinical safety standards to mitigate risks for patients and

Funded by Horizon Europe Framework Programme of the European Union

	staff. Residual risk analysis and documentation
Regulatory Compliance	Validating alignment with local, national, and international medical device regulations: GDPR, MDR/IVDR, ISO 14971 standard

Table 12: Dimensions tested during the validation of the CYLCOMED system

LADS and Dashboard

The LADS and the Dashboard were evaluated in two iterations where patients and volunteers used MCI devices from home. By design, LADS requires an initial training phase to learn the environment. In the first iteration, LADS ran in training mode for 18 hours to model normal traffic patterns. The resulting model then operated in inference mode for 31 days, analysing flows and flagging anomalies.

Because this was a real clinical setting, we could not inject attacks to build a ground-truth dataset. Instead, we used a Cyber Threat Intelligence (CTI) assisted baseline as a proxy. The Dashboard integrated a lookup that, for every flow flagged by LADS, checked whether the public source or destination IP was reported as malicious in VirusTotal or AbuseIPDB. We then assessed LADS using the default threshold for determining predicted anomalies. Confusion-matrix labels were derived by intersecting flows with CTI “malicious” IPs (positives) or not (negatives). This yields a labelled evaluation useful for trend and triage, but not a substitute for curated ground truth.

Dataset and results (*1st iteration*):

- Total flows analysed: 1.946.474
- Predicted anomalies: 68.255
- Predicted non-anomalies: 1.878.219
- CTI-checked public IPs from the analysed dataset: 6.407
    - 4.298 malicious,
    - 2.109 non-malicious.

	Predicted Positive	**Predicted Negative**
Actual Positive (CTI-positive)	33.436 (TP)	0 (FN)
Actual Negative (CTI-negative)	34.819 (FP)	920.859 (TN)

Table 13: Confusion Matrix - LADS 1st Iteration

The metrics calculated for this first iteration were:

Metric	**Formula**	**Result**

Funded by Horizon Europe Framework Programme of the European Union

Accuracy	(TP + TN) / (TP + TN + FP + FN)	96,4%
Precision (PPV)	TP / (TP + FP)	48,99%
Recall (Sensitivity)	TP / (TP + FN)	100%
F1-score	2·(Prec·Rec) / (Prec + Rec)	65,76%

Table 14: Metrics from the 1st Iteration

Within the limits of the CTI proxy, the chosen default threshold achieved very high recall; no CTI-flagged malicious IPs were missed during the 31-day window, at the cost of moderate precision (about half of raised alerts aligned with CTI “malicious” indicators). The high overall accuracy reflects the strong class imbalance (most traffic is benign). False positives likely include legitimate public services and transient behaviours learned during only 18 hours of training.

Although the pilot ran in a real hospital environment behind a firewall with strict geo-based restrictions (limited access from specific countries), LADS still flagged numerous inbound anomalies originating from external sources. Firewall rules blocked these attempts, but LADS provided independent visibility of hostile activity reaching the perimeter. This demonstrates the value of LADS as a defence-in-depth sensor: it validates firewall effectiveness and helps refine allow/deny policies, without exposing clinical systems.

After the joint review with OPBG’s cybersecurity team in Iteration 1, we confirmed the results and spotted internal hospital IPs showing anomalous behaviour. Because the CTI baseline only labels public IPs, those internal findings were not counted as true positives, which affects precision. However, from the internal anomalous flows, we did count some specific cases of

Funded by Horizon Europe Framework Programme of the European Union

bursts of DNS and LDAP communications as true positives, by confirming with the OPBG's team that such a high anomalous volume of DNS and LADS was not normal.

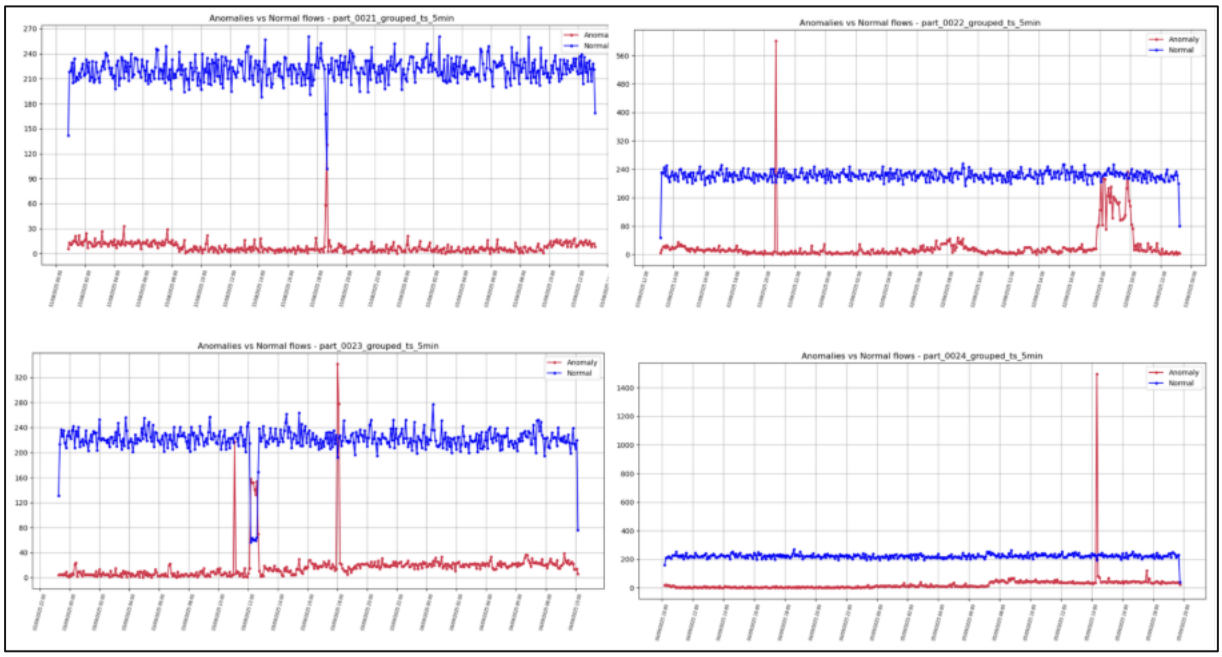

Figure 13 LADS Anomalies vs Normal Traffic (num. of normal vs malicious flows) – OPBG (It. 1)

The figure above shows the flow-level telemetry with short, sharp spikes of anomalies. Together with OPBG's cybersecurity team, we confirmed these bursts were caused by local behaviour such as the LDAP authentication service misbehaving and containers that, for brief periods, restarted repeatedly, generating a surge of ARP traffic. Both patterns legitimately triggered LADS and appeared as anomaly peaks in the timeline. In this first iteration of the

Funded by Horizon Europe Framework Programme of the European Union

OPBG pilot, most malicious traffic was found to originate from the United States and Italy (Figure 33).

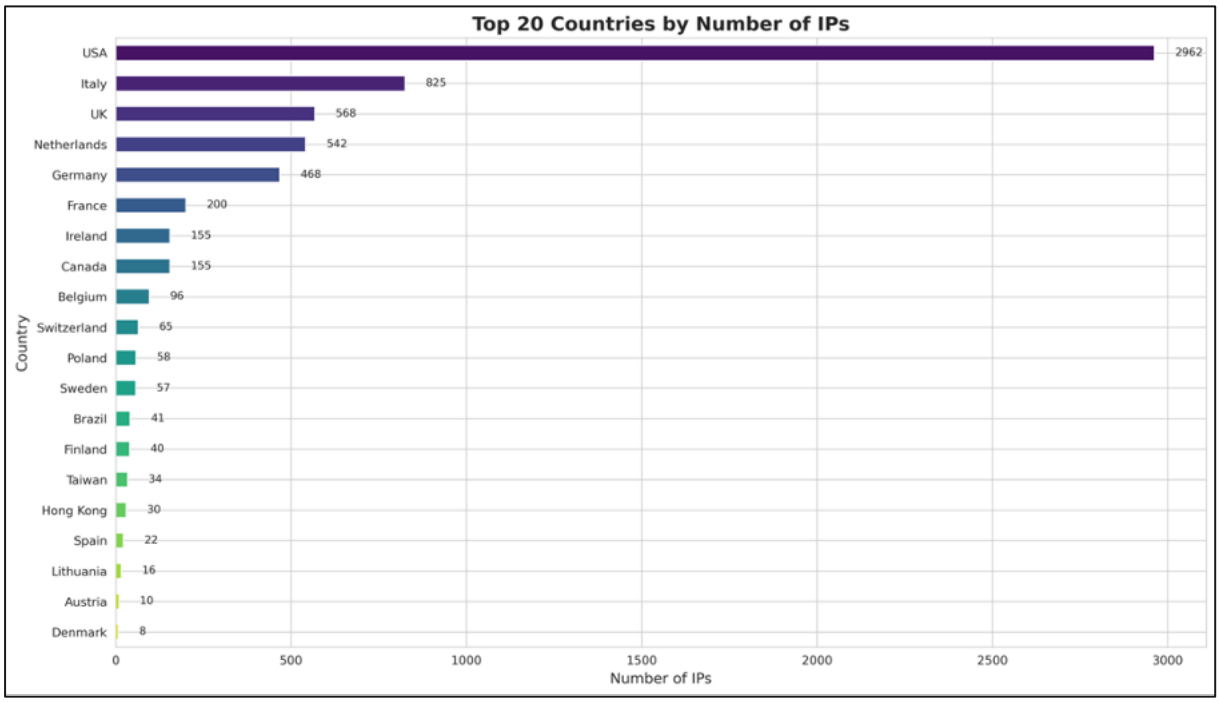

Figure 34: Top 20 Countries - OPBG (It. 1)

Approximately one-third of the processed traffic showed no malicious background, while two-thirds of the IPs had previous reports in AbuseIPDB or VirusTotal (Figure 35)

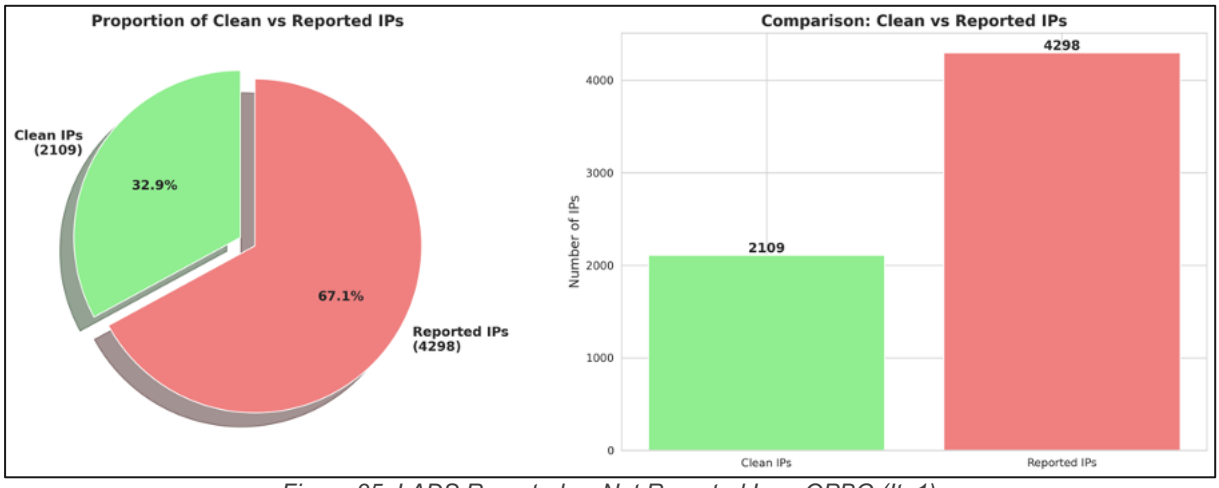

Figure 35: LADS Reported vs Not Reported Ips - OPBG (It. 1)

The most common attack categories associated with these IPs included Port Scanning, Brute Force, and Web Application Attacks, suggesting reconnaissance and exploitation attempts often linked to automated bot activity (Figure 36).

Funded by Horizon Europe Framework Programme of the European Union

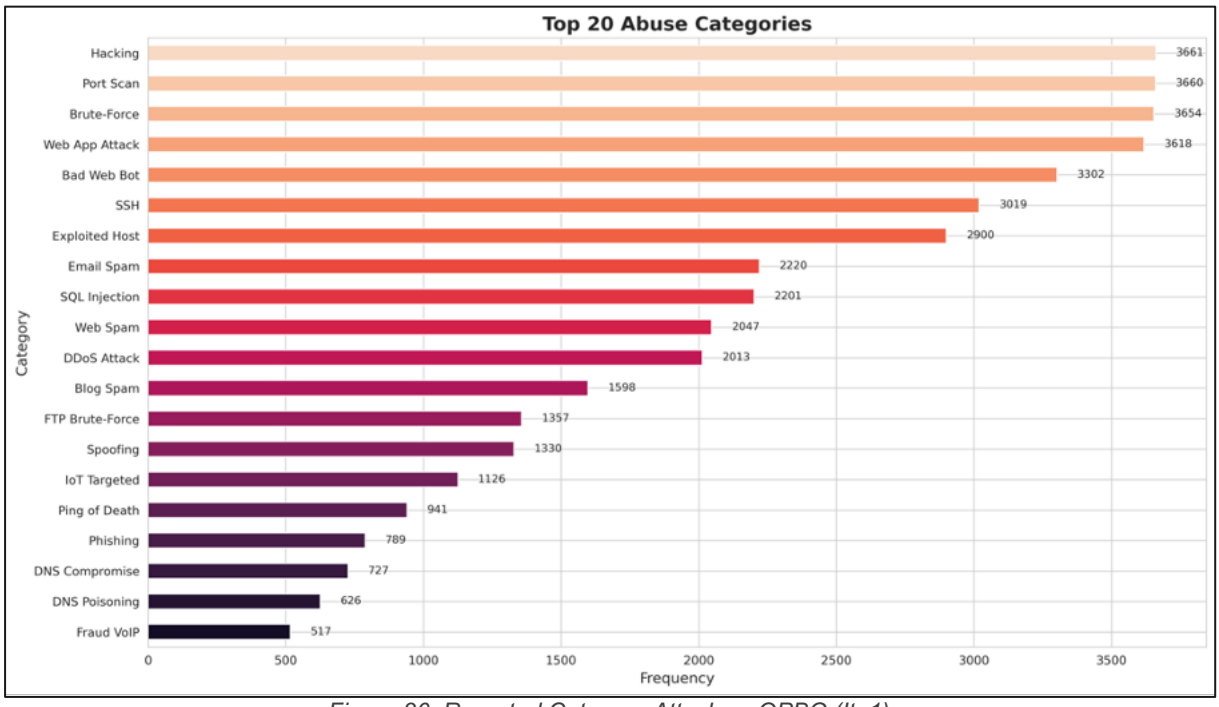

Figure 36: Reported Category Attacks – OPBG (It. 1)

- Total flows analysed: 1.064.723
- Predicted anomalies (RMSE > 10): 34.869
- Predicted non-anomalies: 1.029.854
- CTI-checked public-IP from the analysed dataset: 1.847
    - 1.652 malicious.
    - 195 non-malicious

	Predicted Positive	**Predicted Negative**
Actual Positive (CTI-positive)	15.165 (TP)	0 (FN)
Actual Negative (CTI-negative)	19.704 (FP)	447.575 (TN)

Table 15: Confusion Matrix - LADS 2nd Iteration

The metrics calculated for this last iteration were:

Metric	**Formula**	**Result**
Accuracy	(TP + TN) / (TP + TN + FP + FN)	95,-92%

Funded by Horizon Europe Framework Programme of the European Union

Precision (PPV)	TP / (TP + FP)	43,49%
Recall (Sensitivity)	TP / (TP + FN)	100%
F1-score	2·(Prec·Rec) / (Prec + Rec)	60,62%

Table 16: Metrics from the 2nd Iteration

During this pilot, everything ran in a real hospital network at OPBG, behind strict perimeter controls. Since EVIDEN/ATOS attacks could not be simulated, we chose the approach of using Cyber Threat Intelligence (CTI) from VirusTotal and AbuseIPDB as our only "ground truth" for public IPs. Due to the approach followed, when LADS flagged anomalous traffic from internal hospital IPs (source and destination), those findings could not be confirmed by CTI and therefore counted as false positives in the metrics, even though OPBG's team later confirmed several were genuinely suspicious.

In the first iteration, we analysed 946.474 flows over a longer window, and LADS flagged 68.255 anomalies (RMSE ≥ 10). Besides the metrics shown in the table above, we also saw external anomalies that the hospital firewall had already blocked by policy. This shows LADS detects hostile activity at the perimeter even if it is filtered.

In the second iteration, after retraining and using a shorter observation period, we analysed 1,064,723 flows, and LADS flagged 34,86 anomalies. From the first iteration to the second, Recall remained 1.0, and all flows with source or destination IP that was labelled by CTI as malicious were caught. The drop in precision is explained by CTI's inability to validate internal anomalies, which are operationally meaningful but still scored as FP, and the shorter window producing fewer CTI-labelled malicious contacts (lower TP) while LADS continued to surface suspicious activity.

In this iteration, we observed a substantial increase in the proportion of malicious IPs, with nearly 90% of all identified IP addresses being previously reported as suspicious or malicious (Figure 37)

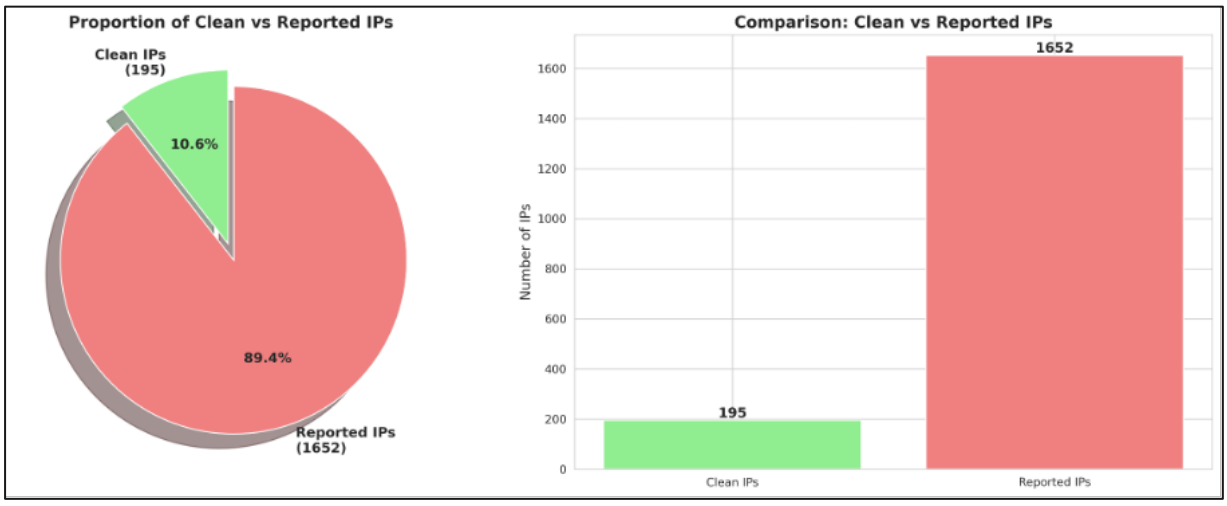

Figure 37: Reported vs Not Reported IPs - OPBG (It. 2)

The geographic origin remained similar to the previous period, with the United States and the United Kingdom being the most frequent sources (Figure 38).

Funded by Horizon Europe Framework Programme of the European Union

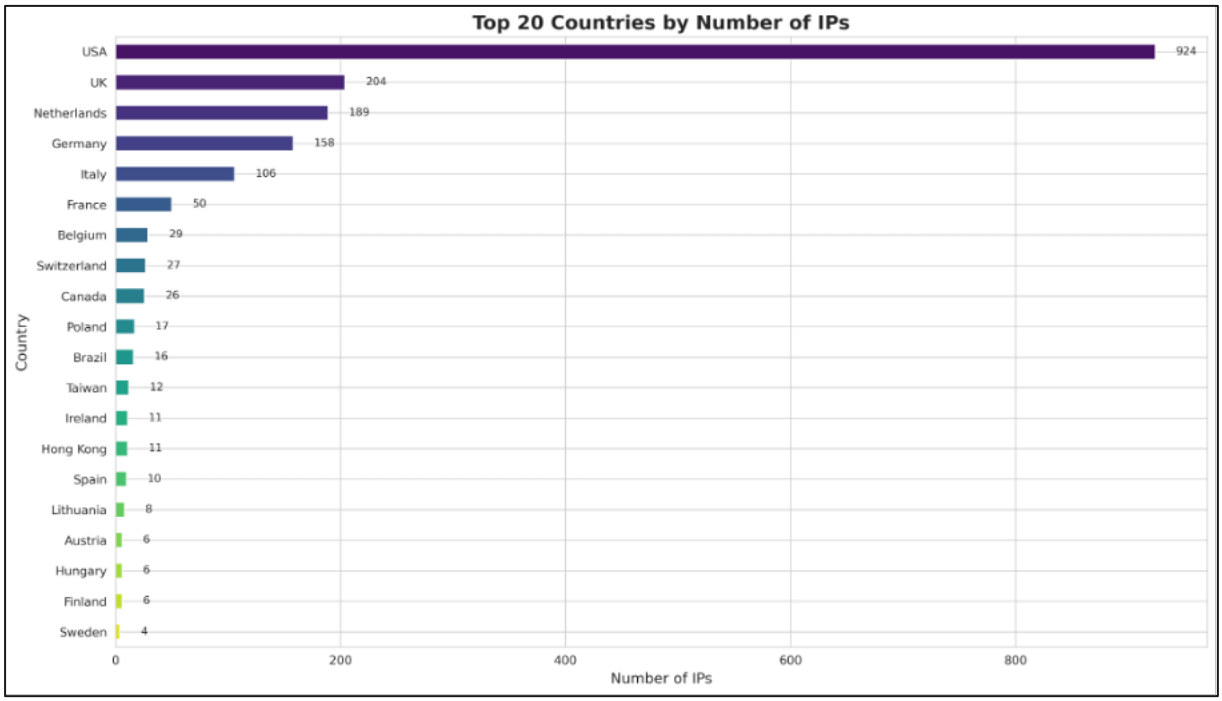

Figure 38: Top 20 Countries - OPBG (It. 2)

The dominant attack types continued to be Port Scanning and Brute Force, indicating persistent automated campaigns aimed at identifying exposed services and exploiting weak authentication mechanisms (Figure 39).

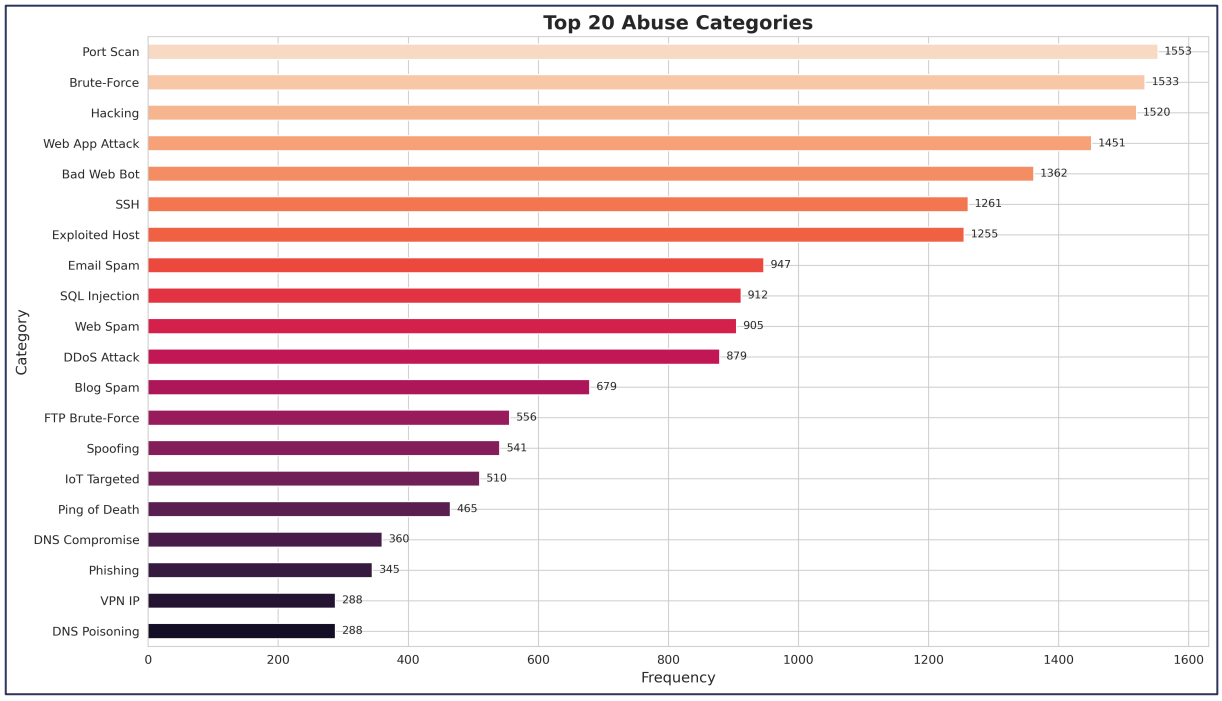

Figure 39: Reported Category Attacks - OPBG (It. 2)

In parallel, we observed a set of flows that LADS consistently flagged as anomalous over time. By design, LADS treats these as true positives from a behavioural standpoint. However, because this was a real hospital environment, we could not craft a labelled ground truth. To approximate one, we cross-checked public source/destination IPs from LADS anomalies against CTI sources (VirusTotal and AbuseIPDB) and counted as “true positives” only those flows involving IPs also reported as malicious externally. This approach is conservative and

Funded by Horizon Europe Framework Programme of the European Union

explains the precision impact: some externally malicious IPs fell outside the accessible reporting window of those APIs (typically ~30 days), so they were not recognised as malicious at query time even when LADS telemetry clearly indicated anomalous behaviour. Those cases were counted as false positives in our scoring, lowering precision while leaving recall high. Additionally, anomalies involving internal hospital IPs (confirmed with OPBG) could not be validated via public CTI and therefore were not counted as true positives in this CTI-based baseline, further biasing results toward higher false-positive counts.

Overall, LADS shows high sensitivity to external threats and useful visibility on internal anomalies. As part of the organic evolution of LADS and Dashboard, it will be necessary to find a way for LADS to easily use SOC annotations and asset allow-lists, adding internal ground truth on each case.

Anomaly period (UTC)	Source IP	Destination IP	Port	Anomaly reason
01/08/2025 09:12:08 -- 09:13:12	44.220.188.44	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.
12/08/2025 18:47:31 -- 18:48:34	44.220.188.199	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.
21/08/2025 05:52:47 -- 05:53:51	98.80.4.75	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.

Funded by Horizon Europe Framework Programme of the European Union

21/08/2025 05:22:07 -- 05:23:10	18.97.5.125	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.
01/09/2025 20:48:19 -- 20:49:12	44.220.188.77	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.
03/09/2025 18:04:25 -- 18:05:28	18.97.26.54	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.
14/09/2025 05:52:53 -- 05:53:56	18.97.26.29	*Local IP*	443(TCP) (TLS)	Potential malicious activity. Unusual number of new sessions/s from unknown/unusual IP address. Opens 10-14 (mostly parallel) sessions per second, total of 600 anomalous sessions for a total duration of approx. 1 min.

Table 17 LADS Results on Samples of Anomalous Flows - External Communication – OPBG

Anomaly period (UTC)	Source IP	Destination IP	Port	Anomaly reason

Funded by Horizon Europe Framework Programme of the European Union

01/08/2025 10:16:23 -- 10:16:30	*Local IP*	*Local IP*	53(UDP)(DNS)	Unusual high number of DNS sessions per second, 110-140 new sessions/s for approx. 7 seconds. All one-directional flows, packets in outgoing direction only.
01/08/2025 10:16:21 -- 10:16:29	*Local IP*	*Local IP*	389(TCP) (LDAP)	Unusual high number of LDAP sessions per second, 50-60 new sessions/s for approx. 6-8 seconds. All one-directional flows, packets in outgoing direction only. Port and LDAP sessions not seen in training.
01/08/2025 10:04:01 -- 10:21:29	*Italian Mobile Operator Public IP*	*Local IP*	443(TCP) (TLS)	95 anomalous flows (sessions) with unusual number of outgoing packets, exceeding (deviating) 700-1500 packets above conformity seen. Likely false positives due to a valid IP address from an Italian mobile operator. A valid normal user communication behavioural validation not seen during training. Requires retraining.
04/08/2025 10:15:44 -- 10:15:49	*Local IP*	*Local IP*	389(TCP) (LDAP)	Unusual high number of LDAP sessions per second, 200 new sessions/s for approx. 5-6 seconds. All one-directional flows, packets in outgoing direction only. Port and LDAP sessions not seen in training.
04/08/2025 10:15:44 -- 10:15:49	*Local IP*	*Local IP*	53(UDP)(DNS)	Unusual high number of DNS sessions per second, 200 new sessions/s for approx. 5-6 seconds. All one-directional flows, packets in outgoing direction only.

Table 18 LADS Results on Samples of Anomalous Flows - Internal Communication - OPBG

For the CYLCOMED pilot conducted at the Hospital Infantil Universitario Niño Jesús (FHUNJ) in Madrid, the deployment topology was more flexible than that of OPBG. Unlike OPBG—

Funded by Horizon Europe Framework Programme of the European Union

where patients interacted with the system from their homes—this pilot relied on volunteers using the MCI medical devices locally in Madrid.

In this scenario, both LADS and the CYLCOMED Security Dashboard were deployed on a dedicated server provided by XLAB and physically hosted in Trento, in proximity to the MCI backend infrastructure. The medical devices in Madrid generated telemetry, which was transmitted over secure channels to the Trento server, where LADS performed local analytics, and the Dashboard provided real-time visualisation.

Throughout the entire pilot period, LADS continuously monitored the network traffic captured from the interaction between the volunteers and the MCI services. The metrics and analysis below refer to a training period of 2.5 days (22/10/2025 07:30h UTC – 24/10/2025 19:30h UTC) followed by an evaluation period of 14.7 days (24/10/2025 19:30h UTC – 08/11/2025 13:00h UTC).

Dataset and Labelling Approach

As in previous pilots, we followed the same CTI-assisted baseline methodology to generate a ground truth baseline and default threshold for the deep leaning models. The obtained dataset:

- Total flows analysed: 4.187.386
- Predicted anomalies (RMSE > 10): 34.730
- Predicted non-anomalies: 3.943.099
- CTI-checked public-IP flows: 177
    - 28 malicious;
    - 149 non-malicious

	Predicted Positive	**Predicted Negative**
Actual Positive (CTI-positive)	24.142 (TP)	0 (FN)
Actual Negative (CTI-negative)	10.588 (FP)	3.913.398 (TN)

Table 19: Confusion Matrix - LADS FHUNJ

The metrics calculated were:

Metric	**Formula**	**Result**
Accuracy	(TP + TN) / (TP + TN + FP + FN)	99,73%
Precision (PPV)	TP / (TP + FP)	69,51%
Recall (Sensitivity)	TP / (TP + FN)	100%

Funded by Horizon Europe Framework Programme of the European Union

F1-score	2·(Prec·Rec) / (Prec + Rec)	82,~~02~~%

Table 20: Metrics FHUNJ Pilot

The FHUNJ pilot displayed a markedly different pattern compared to RGB and OPBG. Only around 15% of the analysed IPs were reported as malicious in AbuseIPDB or VirusTotal (Figure 40), indicating a considerably lower level of detected malicious activity.

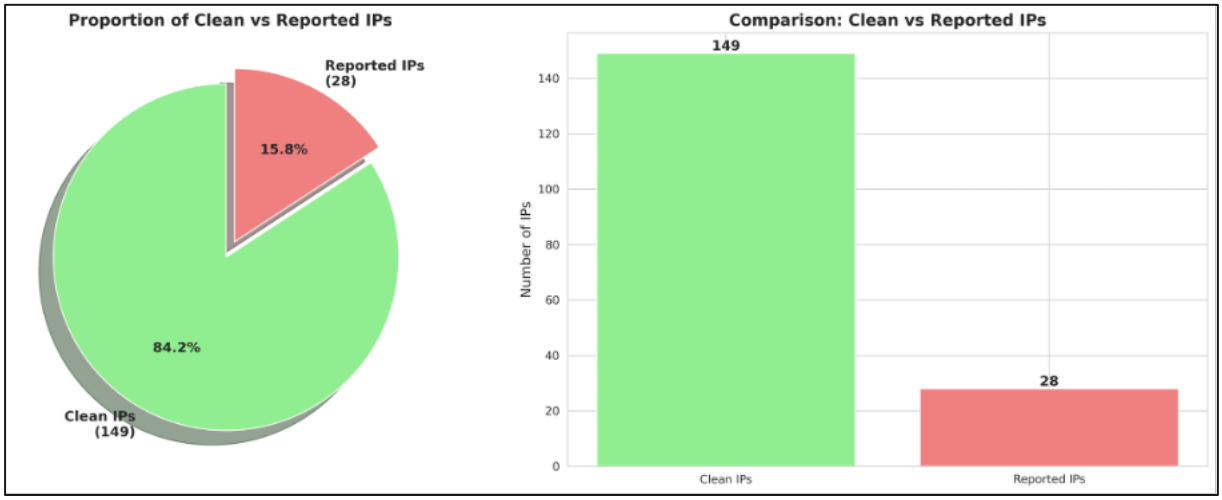

Figure 40: Reported vs Not Reported IPs - FHUNJ Pilot

Among the IPs flagged as malicious, the United States and the United Kingdom appeared as the most frequent countries of origin (Figure 41).

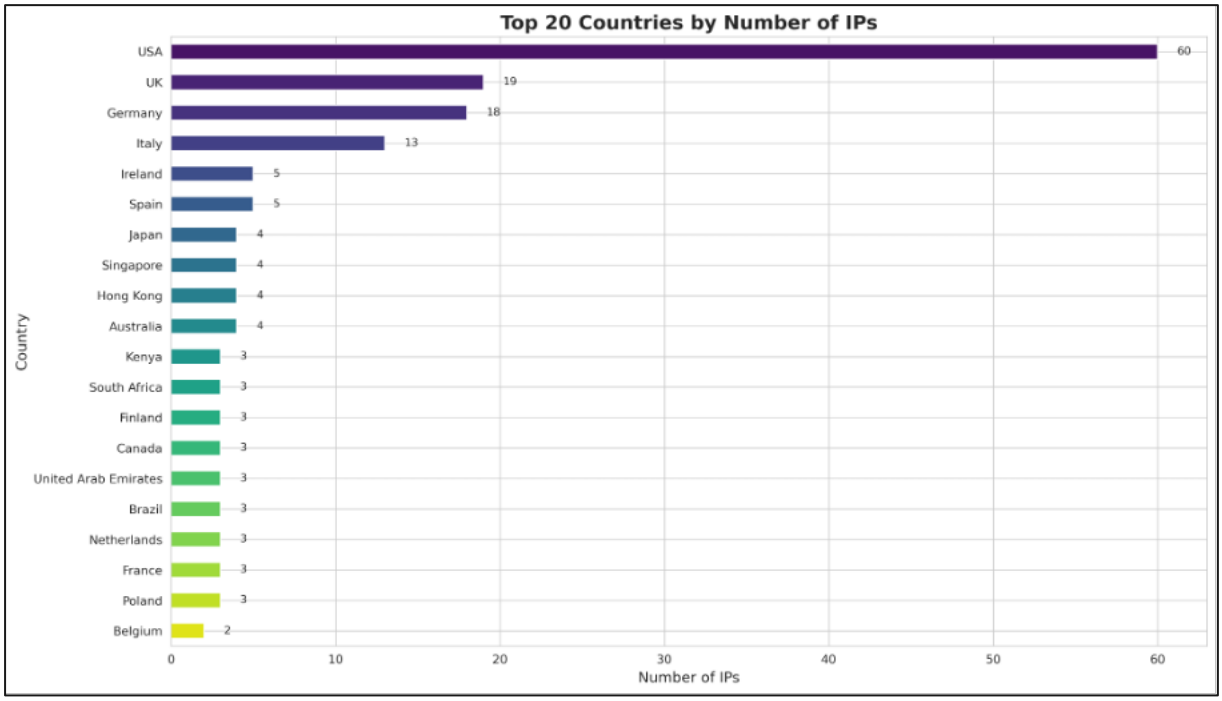

Figure 41: Top 20 Countries - FHUNJ Pilot

The most common attack categories were Port Scanning, Brute Force, and Hacking, which are typical indicators of hostile probing or exploitation attempts (Figure 42).

Funded by Horizon Europe Framework Programme of the European Union

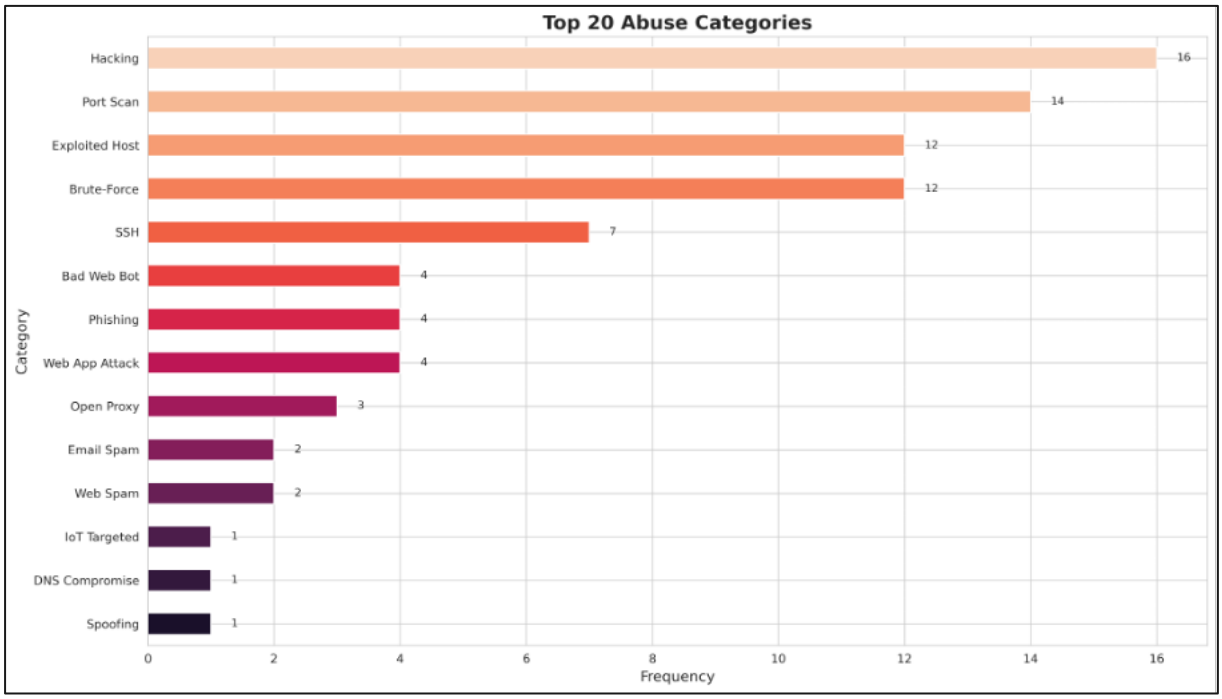

Figure 42: Reported Category Attacks - FHUNJ Pilot

To illustrate the value of LADS, we will briefly describe a set of anomalies, an anomalous behaviour, observed on 30/10/2025 at 14:30h UTC.

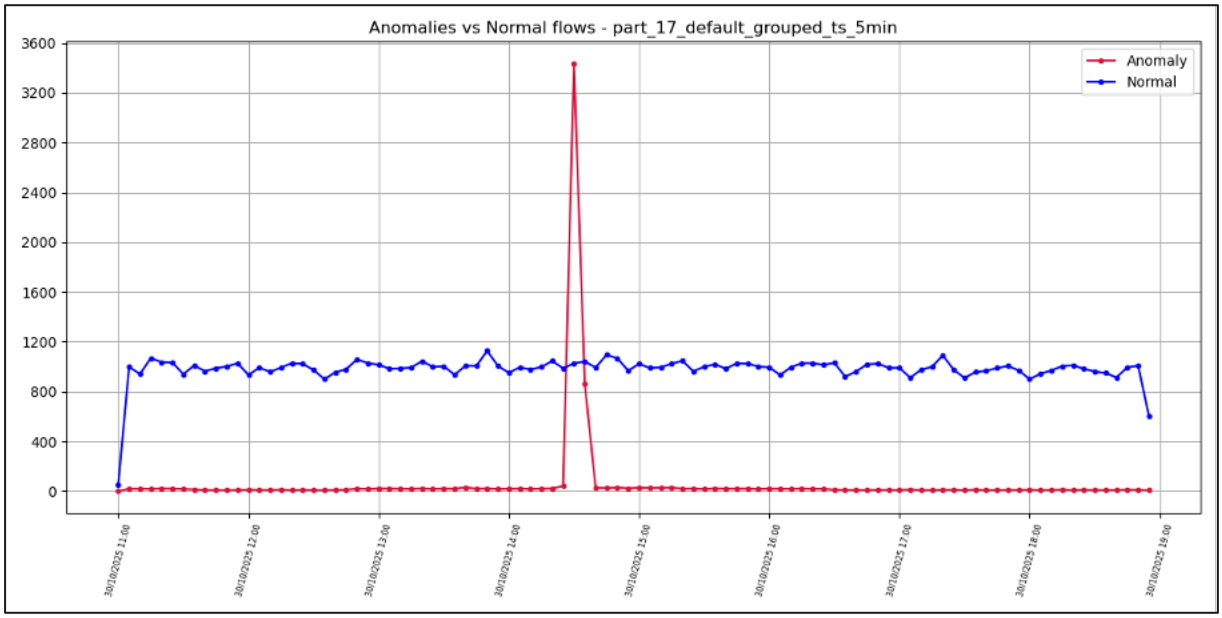

Figure 43: LADS Malicious Activities Detection Flow View – FHUNJ Pilot

Figure shows a sample of flow-level view for a particular anomalous behaviour. While the normal traffic remains constant, there is a surge of anomalous flows (more than 8k) in a short period of time.

Funded by Horizon Europe Framework Programme of the European Union

LOMOS

LOMOS was evaluated using tagged reverse-proxy data from the OPBG hospital, provided by Mediaclinics. We conduct three experiments to assess the model's performance and future-proofing capabilities:

1. Blind test: Training and inference on the full dataset to evaluate basic pattern recognition ability,

2. Full training with recent inference: Using the model trained on the complete dataset (from Experiment 1) but performing inference only on the last 9 days,

3. Temporal validation: Training on all data except the last 9 days, then performing inference on those final 9 days.

By comparing the results of Experiments 2 and 3, we assess how well the model generalizes to future data and determine its suitability for production deployment.

Dataset Analysis

This is a tagged reverse-proxy log dataset, containing 250.000 records with 6 columns, stored in a .csv file, received from MCI. Time range of received data is from July 1, 2025 15:46:36 UTC to July 28, 2025 09:21:01 UTC, about 27 days of log data. Dataset contains 4450 rows tagged as “suspicious“, which is about 1,78% of all logs combined. Log lines contain timestamp in high granularity with microsecond precision, and log entries have a high diversity (247.101 unique entries out of 250.000 records). Their shapes are a standard NGINX "combined" log format structure:

```
$remote_addr - $remote_user [$time_local] "$request" $status
$body_bytes_sent "$http_referer" "$http_user_agent"
```

Schema structure

1. Data Type: All 6 columns are of object dtype (string/mixed type)
2. Index: RangeIndex from 0 to 249,999
3. Completeness: 100% - all columns have 250,000 non-null values

Column Analysis

Column	Description	Unique Values	Data Type
Unnamed: 0	Index/ID field	250.000	Object
ts	Timestamp identifier	146.732	Object
project	Project identifier	2	Object
timestamp	ISO 8601 timestamp	250,000	Object
log	Log message content	247,101	Object
tag	Classification tag	2	Object

Table 19: column analysis

Funded by Horizon Europe Framework Programme of the European Union

Figure 43 presents a chart that shows daily NGINX log volumes and amount of tagged anomalous log lines over 28 days in July 2025, with irregular traffic patterns ranging from under 2.000 to over 25.000 logs per day. The most notable spikes occur on July 2nd, 7th, and 17th.

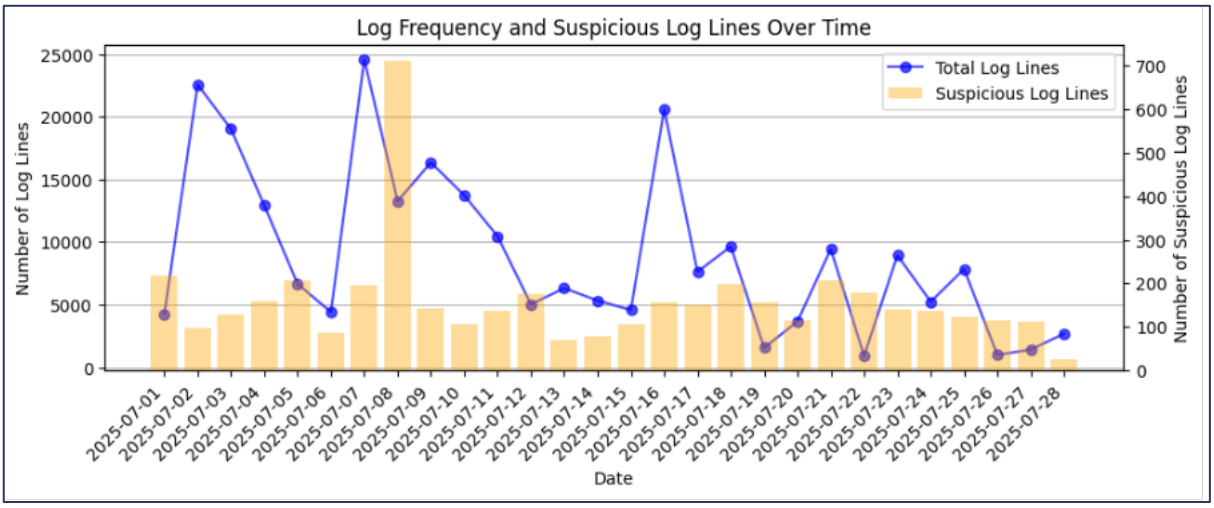

Figure 43: Daily reverse-proxy log volumes

Figure 44 presents a weekly distribution, that reveals a clear business-oriented traffic pattern with Wednesday being the peak day at approximately 69.000 total logs. Weekend traffic (Saturday/Sunday) drops to roughly 25% of weekday volumes.

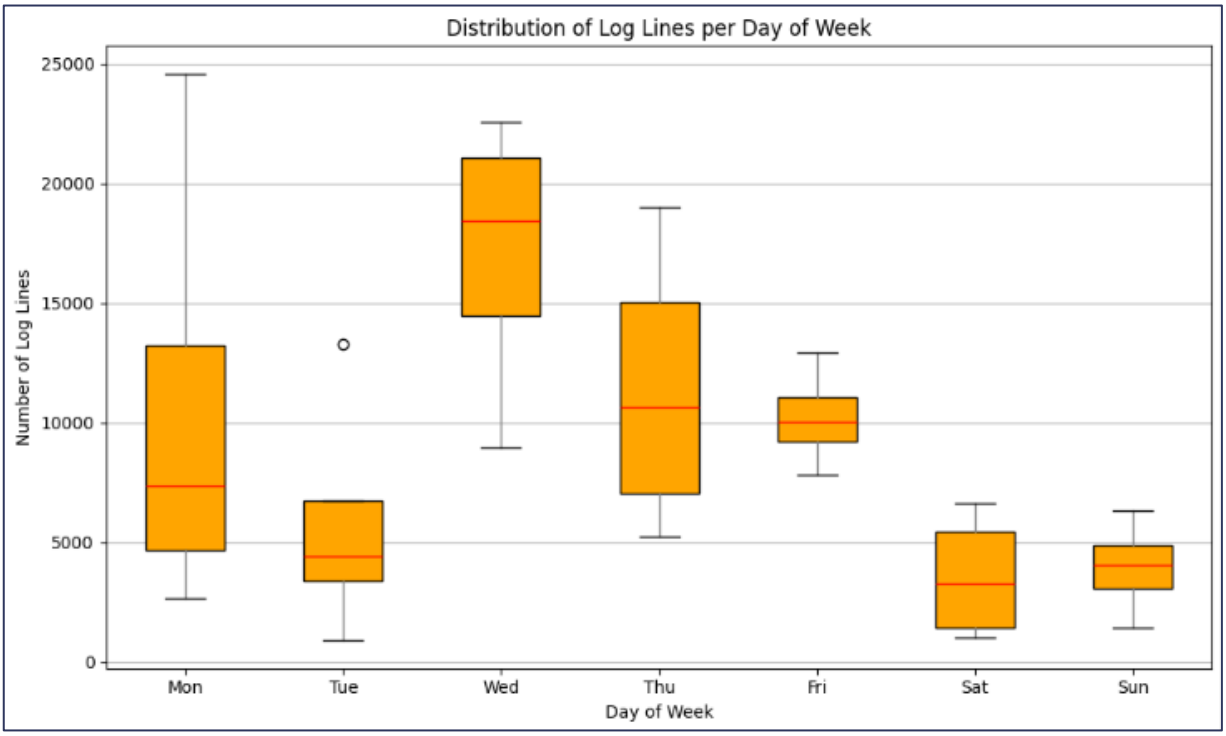

Figure 44: Weekly distribution of reverse-proxy logs

Figure 45 shows the number of log entries generated during each hour of the day, grouped by the hour. At hour 8 (8 AM), there are 46,030 log entries, which is the peak. Early morning hours (0–6) have fewer logs, while activity sharply increases from 7 AM, peaks at 8–9 AM, and then gradually decreases throughout the day, with another small rise in the late evening (21–23). This distribution can help identify periods of high and low system activity.

Funded by Horizon Europe Framework Programme of the European Union

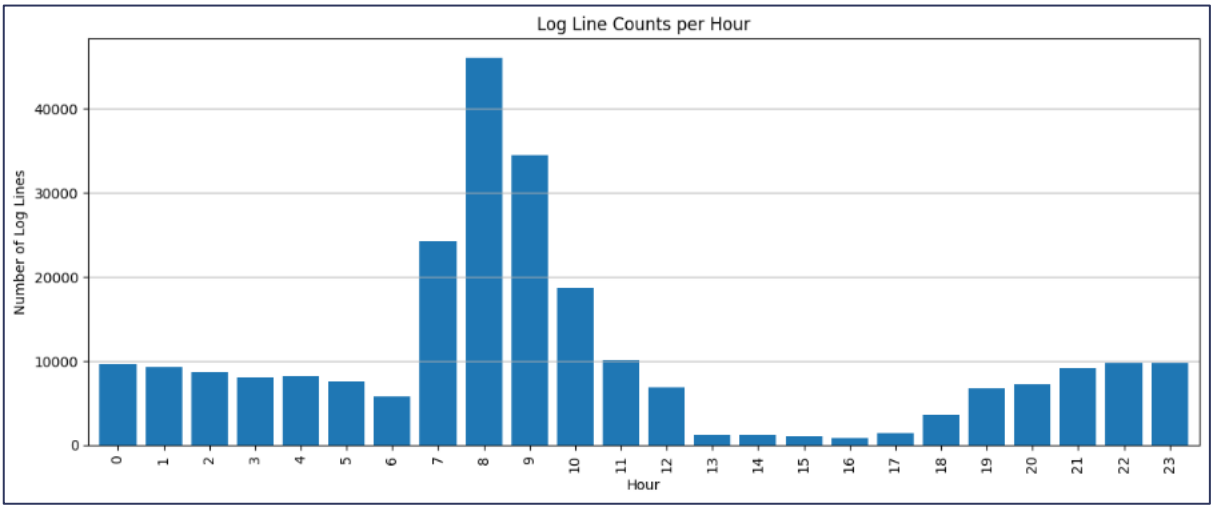

Figure 45: Number of log entries generated during each hour of the day

Experiments

EXPERIMENT 1: Blind test

This experiment evaluated the model's ability to identify patterns when using the complete dataset for both training and inference. The pipeline combined log parsing (Drain algorithm), extensive masking of variable tokens, and a transformer-based anomaly detection model. Used data covers logs from 2025-07-01 15:46:36 to 2025-07-28 09:21:02 (almost one month), total of 250,000 log entries and all of them were used for both training and inference, ensuring consistency in the evaluation and model exposure to the full dataset.

EXPERIMENT 2: Full training, recent inference

The purpose of this experiment was to evaluate how the model trained in Experiment 1 performs when applied only to the most recent data in the dataset, establishing a baseline for recent performance. As mentioned previously, the training data covers logs from 2025-07-01 15:46:36 to 2025-07-28 09:21:02, but inference is performed only on the last 9 days of the dataset, specifically from 2025-07-20 00:00:00 to 2025-07-28 09:21:02.

EXPERIMENT 3: Future-proof test

This experiment was designed to evaluate the robustness of the anomaly detection model on future, previously unseen data. By training the model on historical logs and then testing it on a dataset collected from a later time period, we aimed to simulate real-world deployment conditions where the model encounters new patterns and potential anomalies.

The training period covers logs from 2025-07-01 15:46:36 to 2025-07-20 00:00:00 which counts 208.887 (83,55 %), inference period is between 2025-07-20 00:00:00 and 2025-07-28 09:21:02 logs which is 41.113 (16,44 %) logs.

Results

Experiment 2 was trained on the entire dataset and evaluated on the last 9 days, while Experiment 3 was trained only on data before the last 9 days and then tested on those last 9 days—making Experiment 3 a true test of the model's ability to handle unseen, future data.

Table 15 presents the performance metrics at the optimal thresholds for each experiment. The best values for each metric are highlighted in green, and if the same value appears in multiple experiments, it is highlighted in orange. Only experiments 2 and 3 are compared.

Funded by Horizon Europe Framework Programme of the European Union

	BLIND TEST	FULL TRAINING, RECENT INFERENCE	FUTURE-PROOF TEST
TAGGED LOGS NUM	4450	1156	1156
THRESHOLD	0	0	0
PRECISION	0,7542	0,8475	0,8228
RECALL	1,0000	1,0000	1,0000
F1	0,8599	0,9175	0,9028
ACCURACY	0,7542	0,8475	0,8228
TRUE_POSITIVES	4450	1156	1156
TRUE_NEGATIVES	0	0	0
FALSE_POSITIVES	1450	208	249
FALSE_NEGATIVE	0	0	0

Table 20: Best thresholds per every experiment

At the lowest threshold (0.000), both experiments achieve perfect recall (1.0), meaning all anomalies are detected. However, Experiment 2 achieves slightly higher precision (0,85 vs. 0,82), F1 score (0,92 vs. 0,90), and accuracy (0,85 vs. 0,82), with fewer false positives (208 vs. 249). This is expected, as Experiment 2 has seen all data during training, including the test period, so it can better fit the data distribution.

Experiment 3, on the other hand, is more realistic for deployment: it does not see the last 9 days during training. Despite this, its performance remains strong, with only a small drop in precision, F1, and accuracy. The model still detects all anomalies and keeps false positives at a reasonable level. As the threshold increases, both experiments show the typical trade-off between precision and recall but Experiment 3 maintains competitive precision and F1 scores across a wide range of thresholds.

Several factors can explain these results:

1. **Data Similarity**: The distribution and patterns in the last 9 days are likely similar to the training data, allowing the model to generalize well even to unseen data.
2. **Model Robustness**: The model architecture and training process are effective at capturing the underlying structure of the logs, making it resilient to moderate changes in data over time.
3. **Log Template Stability**: If the log formats and event types do not change significantly between training and test periods, the model will naturally perform well on future data.
4. **Sufficient Training Data**: Having a large and diverse enough training set helps the model learn a wide range of patterns, improving its ability to detect anomalies in new data.

Funded by Horizon Europe Framework Programme of the European Union

5. **Limited Concept Drift**: There may be little to no concept drift (i.e., changes in the statistical properties of the target variable), so the model's learned decision boundaries remain valid.
6. **Effective Preprocessing**: Consistent and thorough preprocessing (e.g., template extraction, normalization) reduces noise and helps the model focus on relevant features.

The fact that Experiment 3's results are close to those of Experiment 2 demonstrates that the model generalizes well and is reliable for detecting anomalies in truly unseen, future data. This increases the chances that the Experiment 3 model suitable for real-world deployment, where new patterns and anomalies will continuously appear.

Evaluation of user experience and usability

To assess the overall usability and user experience of the CYLCOMED cybersecurity Dashboard, a System Usability Scale (SUS) questionnaire [Brooke, John. (1995). SUS: A quick and dirty usability scale. Usability Eval. Ind..189.] was administered to end-users across the partner sites that took part to pilot 1 and 2.

However, since usability is itself an evolving concept, the ways we assess it inevitably depend on how we choose to define it. Nonetheless, it's possible to identify some broad categories of usability measures. According to ISO 9241-11, the usability measures should cover three aspects:

- effectiveness (the ability of users to complete tasks using the system, and the quality of the output of those tasks)
- efficiency (the level of resource consumed in performing tasks)
- satisfaction (users' subjective reactions to using the system)

To properly cover those aspects, the SUS questionnaire has been developed. In fact, it represents a standardized tool for measuring users' subjective perceptions of system usability through a set of ten statements rated on a five-point Likert scale. It can provide a reliable measure for comparing usability across different systems and contexts.

In the CYLCOMED project, the questionnaire was distributed to a representative group of 8, including security managers, IT administrators, clinicians, and developers, representing the key professional profiles expected to interact with the cybersecurity Dashboard. Participants were asked to complete the SUS after gaining practical experience with the platform during the pilot phase.

The analysis of the SUS questionnaire results indicates an overall satisfaction level of 70.9, meeting the project's usability target of >=70%, which correspond to a "good" usability rating according to standard SUS interpretation guidelines. Participants generally perceived the system as easy to use, well integrated, and conducive to rapid learning, as reflected in consistently higher ratings for items addressing ease of use and user confidence. By contrast, lower ratings were observed for statements concerning system interface complexity, highlighting the need for the system to be more user-friendly, thus avoiding the necessity of technical assistance. Minor variability in responses to questions related to consistency and perceived cumbersomeness suggests that some aspects of interface uniformity and operational fluidity could benefit from further refinement. Overall, these findings indicate that the Dashboard's design met user expectations in terms of ease of use, clarity and efficiency.

Funded by Horizon Europe Framework Programme of the European Union

Evaluation of consistency of the platform with requirements after implementation

To assess the effectiveness of the CYLCOMED cybersecurity system, we compared the expectations outlined by the OPBG cybersecurity officer in the context of the initial validation interviews phase, with the actual outcomes observed upon the Dashboard implementation. This comparative approach provides insight into how well CYLCOMED addressed the hospital's cybersecurity priorities and whether it can successfully be integrated with the existing IT infrastructure.

As shown in the following table, the Dashboard met almost all the expectations, with a logic and design that align well with the organization's cybersecurity strategy. Its ability to analyze real-time data and highlight anomalies represents a solid foundation for proactive and real-time monitoring. The comments received provide valuable insights for further growth: enhancing data precision, refining visual clarity, and strengthening algorithm explainability will help build even greater confidence in the system's outputs. Integration with the Security Operations Center (SOC) and existing Security Information and Event Management (SIEM) platforms is seen as the necessary next step to transform the Dashboard from an independent monitoring tool into a component of the incident response process. Overall, the feedback portrays a promising, scalable, and intelligent solution that is steadily evolving toward full operational maturity within the organization's cybersecurity ecosystem.

Pre-implementation expectations	Consistency of the outcomes
System integration with the hospital SIEM system	Dashboard integration requirements align within the hospital IT system such as SOC
Data processing	AI based solution has been developed in CYLCOMED for data processing and decentralization
Continuous monitoring	Real-time analysis 24/7
Good incident detection	Necessity of improvement in the linkage between anomaly detection and incident classification
Rapid incident response Risk-based approach	Real-time risk analysis
Post-incident support	AI based log monitoring

Table 21: Hospital cybersecurity officer expectations and outcomes consistency

3.2.2 Non-technical/clinical Validation of Pilot 2

Method (Interviews)

The non-technical validation process included a structured qualitative component aimed at evaluating user perceptions, ethical considerations, and organizational readiness for the integration of the CYLCOMED cybersecurity toolbox.

Identification of Participants:

For each hospital setting where the CYLCOMED solution was deployed (OPBG, Italy; FHUNJ, Spain), key stakeholders were identified across relevant domains to ensure multidisciplinary coverage. One representative per domain participated in individual semi-structured interviews. The selected participants included:

- Clinicians involved in patient care;

Funded by Horizon Europe Framework Programme of the European Union

- Data Protection Officers (DPOs) responsible for privacy and regulatory oversight;
- Cybersecurity officers managing technical security policies and system integration;
- Supply chain and procurement staff;
- Clinical Trial and Quality Team members overseeing ethical and operational compliance;
- IT/Medical Engineering personnel assessing interoperability and safety of connected systems.

Semi-structured interviews (see Annex A) were conducted in October 2025. A total of 14 interviews were transcribed and analysed thematically to identify recurring concerns, priorities, and expectations for the CYLCOMED toolbox. Analysis focused on five main dimensions: (1) risk perception, (2) asset prioritization, (3) regulatory compliance, (4) usability-security balance, and (5) organizational readiness. Thematic coding followed an inductive process, aligning findings with the project's validation framework and EU regulations such as GDPR, NIS2, and MDR.

Data Analysis:

All interviews were translated into English and analysed using thematic analysis. Transcript data were analysed using GPT-5, an advanced large language model optimized for qualitative data processing through context-adaptive reasoning and multi-layer semantic parsing. The model was employed to perform first-cycle coding, clustering semantically similar responses, and extracting latent themes related to organizational, technical, and ethical readiness dimensions. GPT-5's transformer-based architecture enabled high-resolution token-level comprehension, ensuring contextual coherence across multilingual transcripts while maintaining traceability of coded segments. The analysis workflow combined model-assisted pattern recognition with human-in-the-loop validation, where domain experts reviewed and refined AI-generated thematic maps. This hybrid approach enhanced analytical reproducibility, minimized observer bias, and allowed scalable cross-case comparison between institutional partners. All GPT-5 outputs were version-controlled and benchmarked against manual coding baselines to ensure consistency and methodological transparency, in line with the project's emphasis on trustworthy AI and explainable data analytics. The approach combined inductive and deductive coding to identify recurring patterns across five macro-categories:

1. **Relevance and Perception of Cybersecurity**
2. **Integration and Workflow Usability**
3. **Legal, Ethical, and Societal Readiness**
4. **Procurement and Strategic Value**

System Improvement Suggestions

Patterns were compared across roles to assess convergence and divergence of perspectives. This allowed validation of both the technical and societal dimensions of the CYLCOMED system.

Stakeholder Roles and Value

In order to qualitative asses the real-world relevance of the developed solution, we identified key stakeholders involved in the CYLCOMED ecosystem for their complementary roles and value contribution. Each stakeholder group contributes a distinct but interconnected function within the cybersecurity and digital health framework. Clinicians ensure that technological solutions align with clinical workflows and patient safety, while the Supply Chain unit

Funded by Horizon Europe Framework Programme of the European Union

safeguards procurement integrity and cost-effectiveness. Cybersecurity Officers and Data Protection Officers maintain compliance, risk monitoring, and data governance in line with GDPR and institutional policies. Developers and system integrators enable interoperability and usability, supporting the technical backbone of CYLCOMED. The Clinical Trial and Quality Team guarantees ethical and scientific rigor during implementation, and Medical Engineering and IT Services validate technical robustness and device-level security. Together, these contributions reflect a multidimensional readiness model where technical, ethical, and operational layers coalesce to ensure the secure and sustainable deployment of CYLCOMED across healthcare environments.

Stakeholder	Role Description	Value/Contribution
Clinicians	Healthcare providers involved in direct patient care	Assessed whether cybersecurity tools integrate smoothly into clinical workflows without disrupting care
Supply Chain	Responsible for procurement and sourcing of digital health tools	Evaluated procurement-readiness, contractual compliance, and risk-based cost-benefit factors
Cybersecurity Officer(s)	Managed cybersecurity procedures and technology integration in hospitals	Oversaw implementation and assessed interoperability with hospital IT infrastructure
Data Protection Officer(s)	Ensured compliance with privacy and data protection laws (GDPR, ENS)	Verified regulatory alignment and consent management within the CYLCOMED system
Developers / Technical Integrators	Designed and integrated CYLCOMED software components	Ensured interoperability, usability, and system scalability
Clinical Trial and Quality Team (CTQT)	Supervised research quality, ethics, and IT compliance	Supported legal and ethical conformity during pilot implementation
Medical Engineering / IT Services	Evaluated obsolescence, safety, and performance of medical technologies	Validated technical stability and device-level cybersecurity

Table 22: Hospitals stakeholders' roles and values

Analytical Results and Qualitative Themes

A thematic analysis was used to extract insights from the interviews. Key findings are summarized below.

Relevance and Perception of Cybersecurity

All participants identified cybersecurity as a major concern in the modern hospital ecosystem. They highlighted:

- The growing number of connected medical devices and systems;
- Real-world ransomware incidents disrupting healthcare delivery;
- The critical sensitivity of paediatric patient data.

A clinical engineer stated: "*We no longer think cybersecurity is optional. It must be built-in, especially for devices that monitor patients outside hospital walls*."

Funded by Horizon Europe Framework Programme of the European Union

Integration and Workflow Usability

Clinicians generally perceived CYLCOMED's integration as smooth and non-intrusive but emphasized areas for usability improvement:

- Faster access (e.g., Single Sign-On or biometric login);
- Simplified, intuitive user interfaces;
- Real-time alerts and traceable audit logs;
- Training and update procedures embedded into clinical operations.

As one cardiologist remarked: "*Security is important, but if it adds three extra clicks during clinical work, it's a real problem.*"

Legal, Ethical, and Societal Readiness

DPOs confirmed GDPR and ENS compliance through pseudonymization and audit logs. However, they raised concerns about:

- The granularity of patient consent;
- Explainability and transparency of AI-driven features;
- Risks of unequal access to secure digital care.

The Clinical Trial Lead added: "*Stronger audit trails are needed for compliance and traceability in regulated research*."

Procurement and Strategic Value

Procurement and administrative stakeholders recognized CYLCOMED as a *strategic differentiator* for hospitals aiming at digital transformation, particularly due to its modularity and standard-based design.

They recommended providing clearer information on long-term licensing models, total cost of ownership (TCO), and conformity documentation to accelerate adoption.

System Improvement Suggestions

Respondents proposed several enhancements:

- Single Sign-On (SSO) and biometric authentication;
- Voice command or rapid-access modes for clinicians;
- Dedicated cybersecurity training for healthcare users;
- Dashboards displaying real-time cybersecurity system health;
- Enhanced audit log visualization and alert explainability.

Summary of Qualitative Findings

Overall, the findings show variable maturity between units, with technical departments (such as the Cybersecurity Office and CTQT) reporting high readiness due to established protocols and data-protection infrastructures, while clinical and support functions demonstrate medium to moderate readiness linked to usability constraints, workflow integration, and training needs. The consistent emphasis on AI-based anomaly detection, secure access management, and staff education indicates that the project partners recognize both technological and human-factor challenges. These insights directly inform the readiness assessment presented in the

Funded by Horizon Europe Framework Programme of the European Union

following section, highlighting where targeted actions can strengthen systemic resilience before full deployment.

The comparative overview across departments demonstrates that cybersecurity readiness within the CYLCOMED consortium is heterogeneous but strategically aligned. Departments directly responsible for compliance and technical safeguards, such as the DPO and Cybersecurity Office, exhibit higher maturity due to established GDPR frameworks, proactive risk monitoring, and the integration of privacy-by-design principles. Conversely, clinical and support departments reveal moderate to basic readiness, reflecting limited exposure to cybersecurity governance and the competing demands of clinical workflow efficiency. The data underscore the critical interdependence between human factors, technological preparedness, and organizational policy. Bridging these differences requires targeted capacity-building initiatives, harmonized data-protection protocols, and sustained cross-departmental communication. In essence, the table illustrates a consortium transitioning from compliance awareness to operational resilience, evidencing tangible progress toward a unified cybersecurity readiness model across CYLCOMED.

Department	Core Cybersecurity Concern	Key Assets to Protect	Perceived Maturity	Main Need / Gap
DPO (Data Protection Officer)	Data breaches, ransomware, insider threats, data leaks, phishing	Electronic Health Records (EHRs), IT infrastructure, IoMT	Moderate/strong legal focus	Compliance with GDPR + ENS and privacy-by-design implementation
Cybersecurity Office	Ransomware, data exfiltration, operational disruption	IT infrastructure, medical devices	Fairly mature	Integration, monitoring logs, AI anomaly detection, training
Clinicians	Data leaks, phishing, usability vs. security	EHRs, web systems	Basic awareness, limited training	User-friendly systems, faster secure authentication
Clinical Engineering	Device malfunction via cyberattack	Connected medical devices (IoMT)	Medium	Device protection and interoperability safeguards
Supply Chain	Data breach affecting suppliers	Contractual data, supplier systems	Moderate	Supplier compliance, continuous updates, training
CTQT (Clinical Trials / Quality Team)	Data leaks in telemedicine and trials	Clinical trial data, patient records	High awareness	Encryption, access control, remote monitoring compliance

Table 23: Non-technical validation qualitative findings

The comparative analysis between OPBG and FHUNJ highlights both convergence and divergence in cybersecurity readiness and innovation culture. While both institutions operate within robust European regulatory frameworks, FHUNJ demonstrates a more structured and compliance-driven approach, reflecting Spain's integration of ENS (Spain Esquema Nacional de Seguridad) and LOPDGDD (Organic Law on Protection of Personal Data and Guarantee of Digital Rights) requirements. OPBG, in contrast, shows a more pragmatic stance, balancing legal obligations with innovation and clinical flexibility. Training and awareness emerged as key differentiators: FHUNJ has formalized programs but faces gaps in staff participation, whereas OPBG's initiatives remain fragmented but adaptable. Technically, both institutions

Funded by Horizon Europe Framework Programme of the European Union

exhibit maturity, with OPBG piloting AI-enabled monitoring and FHUNJ advancing infrastructure-based safeguards. Overall, the findings confirm a shared trajectory toward high readiness, yet underline the need for harmonized governance, shared learning, and continued cross-partner alignment to ensure consistent deployment standards across the CYLCOMED network.

Interpretation of qualitative results

The qualitative validation confirmed the high relevance and acceptance of CYLCOMED's cybersecurity system in paediatric telemonitoring and hospital integration. Stakeholders recognized its alignment with regulatory standards, clinical workflows, and institutional governance models.

Key improvement areas include interface usability, faster authentication, and transparent data handling processes.

Aspect	Stakeholder Insights	Implication for CYLCOMED
Integration	Systems must operate "in the background" (Clinical Eng., Cyber Office)	Seamless, non-intrusive integration into hospital IT
Usability vs. Security	Clinicians demand speed (clinical context)	Adaptive security: risk-based authentication or context-aware access
Training	Low cybersecurity literacy among clinical staff	Mandatory phishing awareness, onboarding sessions
Incident Response	Desire for automated logs and immediate alerts	Include post-incident Dashboards and compliance-ready reports
Ethics & Privacy	Consent, ownership, and patient trust emphasized	Transparent consent workflows, anonymization validation

Table 24: Implications of stakeholders' insights for CYLCOMED system implementation

The interview findings triangulate the technical results, showing that CYLCOMED's architecture aligns with operational priorities across roles. Clinicians emphasized emergency-grade access with minimal friction; cybersecurity officers prioritized continuous, explainable anomaly detection and SIEM/SOC integration; DPOs focused on consent traceability, audit logs, and proportionality under GDPR/ENS. These insights confirm CYLCOMED's dual value proposition: (i) technical resilience (continuous monitoring, encryption, identity/authorization), and (ii) clinical adoptability (usability, workflow fit, and governance).

Funded by Horizon Europe Framework Programme of the European Union

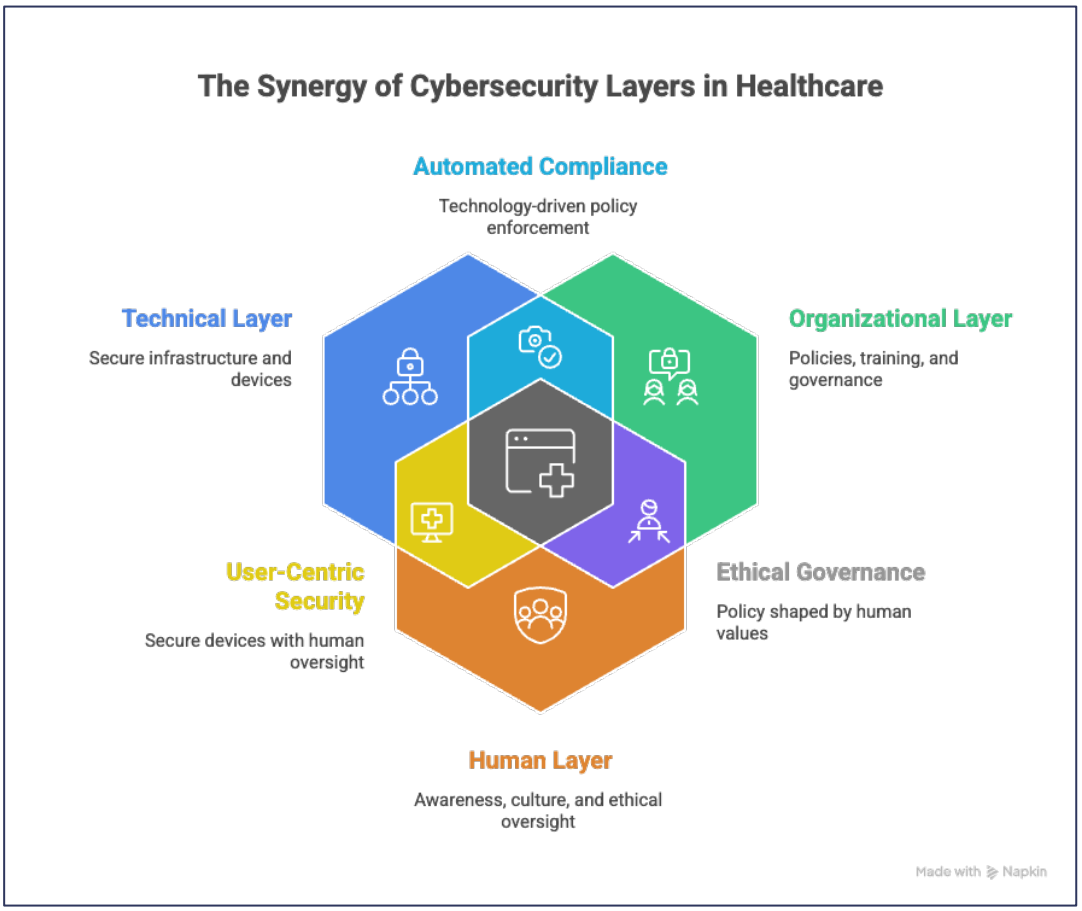

Figure 46: Multilayer cybersecurity framework of the CYLCOMED project. The model integrates four complementary layers—technical, analytical, privacy-by-design, and governance—to ensure end-to-end protection of connected medical devices. AI-driven monitoring and continuous training operate alongside compliance to safeguard patient safety and trust.

The results highlight the project's readiness for institutional scaling and its potential to serve as a reference framework for secure, ethically sound digital health transformation across Europe. Interestingly, Procurement stakeholders viewed the toolbox as a strategic differentiator if bundled with clear conformity evidence, TCO/ROI projections, and integration guidance (SOC/SIEM, identity providers).

These findings strengthen the evidence that CYLCOMED's approach—combining AI-assisted detection, privacy-by-design, and human-centered design—supports both **compliance** and **clinical adoption.**

Families' cybersecurity risk perception - Survey

Given the increasing digitalization of clinical data, cybersecurity has taken on a new level of importance, particularly in paediatric care where families often have limited awareness of the risks related to the handling of their children's health information. To better understand parents' perceptions of these risks, a dedicated, anonymous questionnaire was developed and administered to 64 families visiting OBG hospital during the final piloting phase at Bambino Gesù Children's Hospital (OPBG). The questionnaire, composed of seven closed-ended questions, aimed to explore families' habits around data protection, their willingness to share clinical information, their trust in the healthcare system, and the value they place on transparency in data management. This activity aligns with CYLCOMED's broader objective

Funded by Horizon Europe Framework Programme of the European Union

of fostering a user-inclusive approach to cybersecurity in healthcare, ensuring that not only clinical and technical stakeholders, but also patients and caregivers, are actively engaged in the design, implementation, and evaluation of secure digital health solutions.

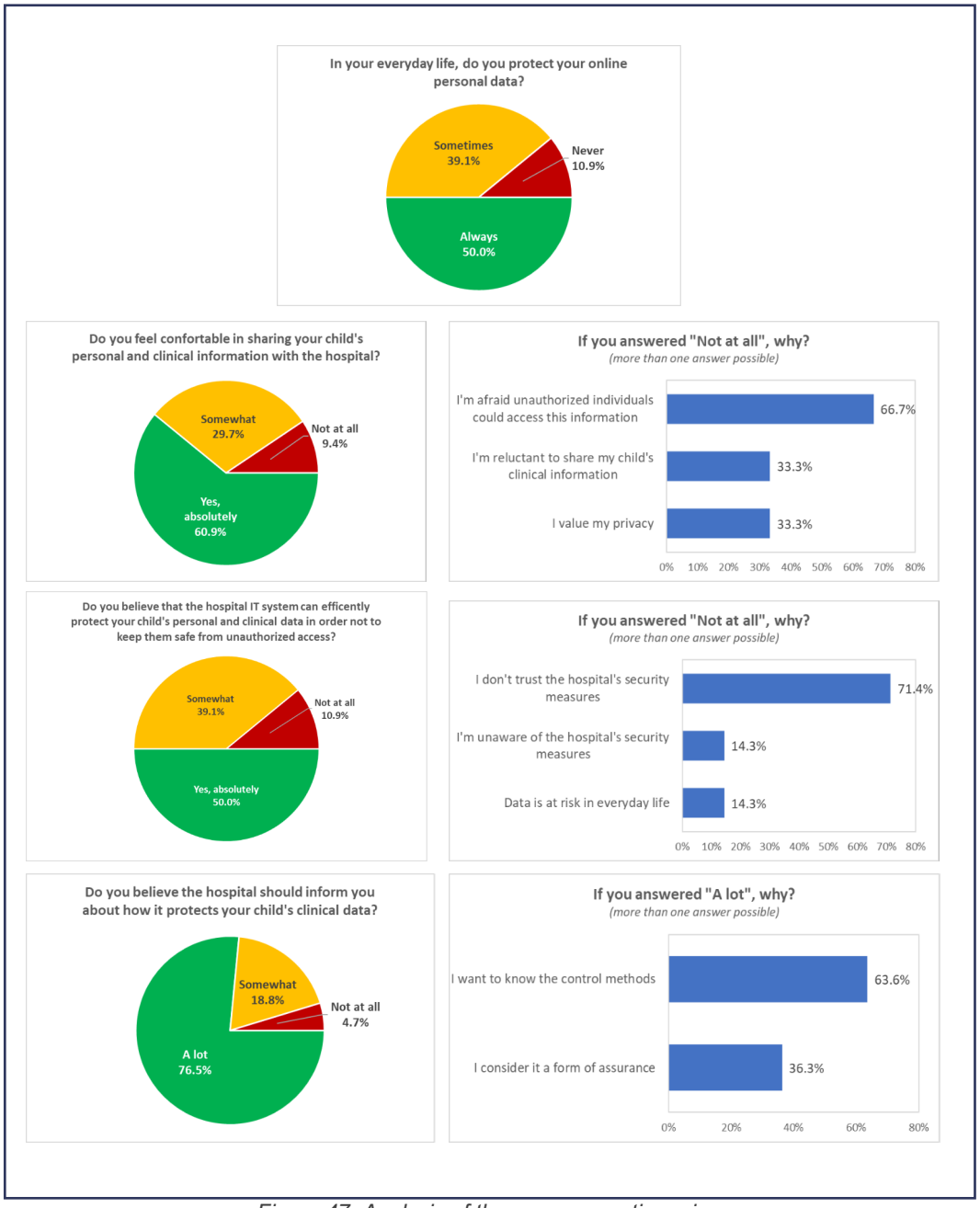

Figure 47: Analysis of the survey questionnaire

The survey (Figure 47) shows that parents of paediatric patients generally understand the importance of protecting health data, even if most lack a detailed grasp of cybersecurity mechanisms. Trust in healthcare systems is moderate to high, with about half of families relying on institutional protections. However, over 10% of parents admit to taking no personal protective measures, and a similar proportion express concerns about potential data misuse or theft.

A strong message emerging from the results is the demand for transparency: nearly 80% of respondents want not just reassurance that their data are secure, but also a clear explanation

Funded by Horizon Europe Framework Programme of the European Union

of how this security is achieved. This highlights the need for open, accessible communication about data protection, particularly in paediatric settings.

The survey underlines that cybersecurity is a crucial dimension of patient safety. Lack of awareness or poor digital practices can expose patients to real risks, from privacy breaches to disruptions in care. Collaboration between IT and clinical professionals remains limited, leaving gaps in the protection of connected medical devices and telemedicine platforms, areas increasingly vital in modern healthcare.

Interpretation of validation results

The validation process of Pilot 1 was carried out in RGB premises under laboratory conditions. The landscape of medical equipment has revealed to be experimenting a considerable evolution, and the CYLCOMED tools have proved to be effective; the technical solution used in implementation has proved that it does not affect the performance of the original medical system, which proves that the use of an RPI external board has enough CPU power to cope with additional cybersecurity related work. Besides, the solution is good to simplify the equipment recertification issues.

The final-phase validation of the CYLCOMED cybersecurity toolbox reveals a system that is technically effective and strategically aligned with clinical workflows. The integration of CYLCOMED into real-world hospital contexts allowed stakeholders to evaluate not only its functionality and safety but also its ethical robustness, usability, and long-term procurement potential.

A key strength of CYLCOMED lies in its bottom-up, human-centred validation strategy. In contrast to purely standards-based frameworks, the project engaged clinicians, engineers, data protection officers, and quality managers in structured interviews, uncovering both enablers and barriers to adoption. These included the need for streamlined emergency access, clearer patient communication, and transparent data governance.

CYLCOMED stands out not only as a technical solution but as a translational framework for ethical, scalable, and context-aware digital security in healthcare. Its validation in real-world scenarios such as paediatric care setting underscores the importance of designing with users and patients—not just for them. The findings from Pilot Sites provide a solid foundation for broader deployment across Europe and offer a reproducible model for responsibly embedding cybersecurity into connected medical ecosystems.

Comparing CYLCOMED with WHO 2025 Framework

In assessing the broader significance of these findings, it is useful to contrast CYLCOMED's validation strategy with the WHO 2025 Cybersecurity and Privacy Maturity Model [WHO/EURO:2025-11827-51599-79106], which offers a top-down, standards-based approach for assessing institutional readiness. While the WHO model emphasizes policy, governance, and benchmarking maturity across six core domains (e.g., data lifecycle, governance, incident management), CYLCOMED's approach is explicitly bottom-up and user-centric, focusing on:

- Real-time system performance under clinical loads
- Workflow integration and usability from the perspective of clinicians and engineers
- Privacy risk perception and ethical impact, especially in paediatric care contexts
- Validation through stakeholder interviews, rather than only policy audits

This contrast is meaningful. CYLCOMED goes beyond formal compliance to engage directly with the lived experience of healthcare workers using cybersecurity technologies. For example, while the WHO framework references "user behaviour" as a compliance indicator, CYLCOMED directly

Funded by Horizon Europe Framework Programme of the European Union

interrogated this via structured interviews, uncovering both behavioural patterns and usability concerns (e.g., login friction during emergencies).

Notably, CYLCOMED's qualitative insights into trust, patient communication, and workflow fit expand the WHO framework's current emphasis on technical safeguards by adding a societal and human-centered validation layer. This inclusion is particularly critical in pediatric contexts, where ethical scrutiny and caregiver transparency are non-negotiable.

Ethical and Societal Readiness

Interviews with legal and clinical stakeholders also underscored the importance of ethical transparency in cybersecurity systems. Several respondents emphasized the need to better explain how the system handles data access, anonymization, and synthetic data usage—topics often neglected in traditional maturity models. Furthermore, stakeholders raised concerns about unequal access to secure telemonitoring technologies, urging designers to anticipate future disparities in digital healthcare protection.

By incorporating these insights, CYLCOMED's validation process goes further than proving "compliance"—it explores whether the system genuinely supports safe, equitable, and human-centered digital care.

Implications for Scale-Up and Procurement

The positive reception from the procurement team—who viewed the toolbox as a potential strategic differentiator—is particularly encouraging. Their request for clearer documentation (e.g., conformity statements, ROI projections) indicates that while technical and clinical value is recognized, market readiness materials must now follow.

To facilitate wider adoption, CYLCOMED could benefit from adopting selected WHO-style benchmarking elements (e.g., radar plots, 1–4 scoring scales) to visually communicate its maturity and alignment with global standards. This would bridge the strengths of both frameworks and support regulatory alignment and institutional trust-building.

Funded by Horizon Europe Framework Programme of the European Union

4 Conclusions

Through the pilots, the project has put into practice a structured cyber risk management framework, specifically designed for CMDs and the novel technologies they increasingly rely on, such as AI, taking into account the acceptability of stakeholders, the consistency with existing policies and the integration in real world conditions. These validation activities support the broader goal of developing a comprehensive, standards-aligned toolbox that can be realistically implemented within healthcare infrastructures.

Crucially, this report feeds into the continuous refinement of cybersecurity guidelines, standards and best practices, incorporating findings from the field and aligning them with ongoing legal, ethical, and regulatory analyses conducted by the project. By observing how the toolbox performs in live settings, the pilots may contribute to evidence-based recommendations aimed at improving the regulatory and ethical frameworks that govern cybersecurity for CMDs.

Finally, the insights gathered here directly support CYLCOMED's commitment to maximising its impact through dissemination, exploitation, and training. The lessons learned in this final stage not only validate the technical solutions, but also reinforce strategies for stakeholder engagement, capacity building, and long-term adoption across Europe's digital health ecosystem.

Funded by Horizon Europe Framework Programme of the European Union

5 Annexes

5.1 A: Questionnaires used for non-technical validation by type of stakeholder

Clinicians

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	Do you have any concerns about how patient data is handled or accessed in your department?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	
5	Do you expect the CYLCOMED cybersecurity system to fit into your daily clinical activities? What are the components of the systems that are more relevant for you?	
6	Do you anticipate any challenges in learning how to use new systems or devices?	
7	What features would you find most useful in a secure telemonitoring platform?	
8	How important do you think it is to protect patient data in your daily practice?	
9	Do you think the CYLCOMED system should prioritize ease of use or security, or balance both? Why?	
10	Are there specific tasks in your workflow where you feel cybersecurity measures may interfere (e.g., authentication, data access)?	
11	Are there any specific tasks in your workflow where you think additional security might create delays or challenges?	
12	How important is it for the CYLCOMED system to have a simple and intuitive interface? Are there specific areas where you feel user-friendly design is crucial (e.g., logging in, data retrieval, emergency access)?	
13	How would you explain the importance of data security to patients who may have questions or concerns?	

Supply chain

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	What level of cybersecurity is acceptable for your specific role/department (e.g., clinical, administrative, IT)?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	

Funded by Horizon Europe Framework Programme of the European Union

5	Do you believe that developing and testing a prototype cybersecurity toolbox could provide a strategic advantage in the hospital's procurement process?	
6	How would you negotiate an agreement for the early adoption of a cybersecurity toolbox developed in a research project?	

Cybersecurity manager

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	What level of cybersecurity is acceptable for your specific role/department (e.g., clinical, administrative, IT)?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	
5	Which functions would you expect in a system for cybersecurity for telemonitoring	
6	What do you expect in terms of the system’s ability to detect, respond to, and recover from security incidents?	
7	How quickly should the system respond to cybersecurity threats or data breaches?	
8	What kind of post-incident support or communication do you expect from the system?	
9	What level of training and ongoing education do you expect to receive about using the CYLCOMED cybersecurity system effectively?	
10	How familiar are you with current cybersecurity protocols, and what improvements do you expect from the new system?	
11	Are there areas where you feel more support is needed (e.g., phishing awareness, handling of sensitive data)?	

Data Protection Office

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	What level of cybersecurity is acceptable for your specific role/department (e.g., clinical, administrative, IT)?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	
5	Which functions would you expect in a system for cybersecurity for telemonitoring	
6	What are the specific regulatory requirements (e.g. GDPR) you are concerned the system should meet?	
7	How do you think the cybersecurity system should address compliance with legal standards?	

Funded by Horizon Europe Framework Programme of the European Union

8	What role do you expect the cybersecurity system to play in ensuring regulatory audits are passed successfully?	
9	How should the cybersecurity system balance data access with privacy concerns?	
10	How do you perceive the use of synthetic data or anonymization techniques to protect patient privacy?	
11	How do you perceive the ethical implications of using a cybersecurity system (e.g., patient consent, data ownership)?	
12	What are your concerns regarding the potential societal impact of the CYLCOMED cybersecurity system (e.g., unequal access to healthcare technology, patient trust)?	

Clinical Trial Quality Center

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	What level of cybersecurity is acceptable for your specific role/department (e.g., clinical, administrative, IT)?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	
5	What is your expectation regarding the economic impact of implementing the CYLCOMED cybersecurity system?	
6	Do you foresee cost savings or increased efficiency due to the system, and if so, how?	
7	How do you define success in terms of return on investment (ROI) for cybersecurity?	

Clinical Engineering

1	What are the primary security concerns you have for the healthcare organization (e.g., data breaches, ransomware, insider threats)?	
2	Which assets or systems do you consider the most critical to protect (e.g., patient records, medical devices, hospital IT infrastructure)?	
3	What level of cybersecurity is acceptable for your specific role/department (e.g., clinical, administrative, IT)?	
4	How do you currently perceive the organization's ability to manage and mitigate cybersecurity risks?	
5	Which functions would you expect in a system for cybersecurity for telemonitoring (adapt to other use cases)	
6	How do you expect the cybersecurity system to integrate with current clinical and administrative workflows?	

Funded by Horizon Europe Framework Programme of the European Union

7	What concerns do you have about the system affecting the efficiency of daily operations (e.g., delays due to security protocols)?	
8	How do you perceive the use of synthetic data or anonymization techniques to protect patient privacy?	
9	What level of ease of use do you expect from the cybersecurity system?	
10	What do you expect in terms of the system's ability to detect, respond to, and recover from security incidents?	
11	How quickly should the system respond to cybersecurity threats or data breaches?	
12	What kind of post-incident support or communication do you expect from the system?	
13	How familiar are you with current cybersecurity protocols, and what improvements do you expect from the new system?	
14	Are there areas where you feel more support is needed (e.g., phishing awareness, handling of sensitive data)?	
15	How do you perceive the ethical implications of using a cybersecurity system (e.g., patient consent, data ownership)?	
16	How do you define success in terms of return on investment (ROI) for cybersecurity?	
17	Are there any challenges you foresee in maintaining compliance with evolving healthcare regulations?	
18	How do you expect the threat landscape to change in the next few years, and how do you plan for adaptability in the system?	
19	How do you expect to collaborate with other departments (e.g., IT, legal, compliance) during the system's development and deployment?	

Funded by Horizon Europe Framework Programme of the European Union