European Commission
Horizon 2020
European Union funding
for Research & Innovation

Horizon 2020 Marie Skłodowska-Curie
Research and Innovation Staff Exchange Evaluations (RISE)

AERAS

A CybEr range tRaining platform for medicAl organisations and systems Security

D5.3: AERAS initial prototype pilot validation report †

Abstract: This deliverable constitutes the main output of Task T5.3 which ensures the deployment and initial validation of the AERAS cybersecurity platform in UPAT's and PAGNI's smart hospital. This phase assesses the platform's integration, usability, and effectiveness in addressing cybersecurity threats, supported by user training through Cyber Range Security Assurance modules. The findings highlight the platform's ability to enhance staff awareness and response capabilities while identifying areas for refinement. Key performance indicators and user feedback establish a baseline for further development toward the final prototype. D5.3 contributes to AERAS's goal of delivering a scalable, resilient cybersecurity solution for healthcare.

Contractual Date of Delivery	30/11/2024
Actual Date of Delivery	31/12/2024
Deliverable Security Class	Public
Editor	Efstratios Syrmas, George C. Kagadis (UPAT)
Contributors	Konstantinos Kalais (CUT) Stella Tsichlaki (PAGNI) Kyriakos Georgiou, Sotirios Chatzis, Katerina Christophidou, Demetres Arnatoutis (CUT) Konstantinos Papadamou, Nikolas Ioannu, Dimitros Donas, Manolis Minaides, Nikoleta Vryoni (TRID)
Quality Assurance	Fulvio Frati (UMIL) Konstantinos Panousis (EAIN)

† *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 872735.*

The *AERAS* Consortium

Universita degli Studi di Milano	UMIL	Italy
Technologiko Panepistimio Kyprou	CUT	Cyprus
Sphynx Analytics LTD	STS-CY	Cyprus
AEGIS IT RESEARCH GMBH	AEGIS	Germany
Panepistimiako Geniko Nosokomeio Irakleiou	PAGNI	Greece
Panepistimio Patron	UPAT	Greece
TRID TRINOMIAL TECHNOLOGIES LTD	TRID	Cyprus
Ethical AI Novelties	EAIN	Cyprus
Libra AI Technologies	LIBRA	Cyprus

Document Revisions & Quality Assurance

Internal Reviewers

1. Fulvio Frati (UMIL)
2. Konstantinos Panousis (EAIN)

Revisions

Version	Date	By	Overview
1.0	31/12/2024	Editor	Final version
0.7	23/12/2024	Editor	Version ready for internal review
0.5	01/12/2024	Editor	Analysis of results and finalization of validation section
0.3	15/11/2024	Editor	Finalization of the questionnaire
0.1	01/10/2024	Editor	First version, including structure of the document

Executive Summary

Deliverable D5.3 presents the initial validation of the AERAS platform, deployed in UPAT's and PAGNI's hospital environment. This phase assesses the platform's integration and effectiveness in detecting and mitigating cyber threats in a realistic healthcare setting. Through hands-on engagement with AERAS's Cyber Range Security Assurance modules, hospital staff trained to identify and respond to simulated cybersecurity scenarios, including phishing, malware, and GDPR compliance incidents. This report details AERAS's initial performance alongside user feedback on usability. Findings identify both strengths and areas for enhancement, forming the basis for ongoing development toward the final prototype and supporting the platform's goal of improving cybersecurity resilience in healthcare.

Table of Contents

1. Introduction 8
1.1 Role of the Deliverable 8
1.2 Relationship to other Deliverables 8
1.3 Structure of the document 9
2. Pilot Deployment Framework 11
3. System Readiness, User Training and Familiarization 13
3.1 Objectives of CRSA-driven Training Programs Role of the Deliverable 13
3.2 Training Materials and Delivery Methods 16
3.3 Structured Onboarding Process 17
4. Comprehensive Evaluation and Recommendations for the Initial Prototype Pilot 19
4.1 Overview of Evaluation Phases 19
4.2 Key Findings on System Performance 20
4.3 Adherence to Cybersecurity Compliance Requirements 21
4.4 Identified Technical Issues and Defect Resolution 22
4.5 Platform Improvements Based on User Feedback 23
4.6 Scalability and Replication Potential 24
4.7 Key Milestones for Further Development 24
5. Conclusions 25
5.1 Primary Insights from Pilot Evaluation 25
5.2 Contribution of D5.3 to AERAS Goals 25
6. Annex A: AERAS Cybersecurity Questionnaire 27

List of Figures

Figure 1: Pie chart of percentage of responses to the question: Have you received formal training or certification related to cybersecurity? 13
Figure 2: Pie chart of percentage of responses to the question: How confident are you in complying with regulations like GDPR or other healthcare data privacy laws for protecting patient information? 14
Figure 3: Pie chart of percentage of responses to the question: How familiar are you with ransomware and the procedures to follow in case of a ransomware attack? 14
Figure 4: Pie chart of percentage of responses to the question: How often do you update your passwords? 15
Figure 5: Chart of percentage of responses to the question: Have you or your team encountered any of the following cybersecurity issues? 20
Figure 6: Chart of percentage of responses to the question: What additional cybersecurity training or support would you find beneficial in your role? 23

Table of Abbreviations

AERAS	A CybEr range tRaining platform for medicAl organisations and systems Security
CRSA	Cyber Range Security Assurance
UPAT	University of Patras
PAGNI	Panepistimiako Geniko Nosokomeio Irakleiou
UMIL	Universita degli Studi di Milano
CUT	Technologiko Panepistimio Kyprou
STS-CY	Sphynx Analytics LTD
AEGIS	AEGIS IT RESEARCH GMBH
TRID	TRID TRINOMIAL TECHNOLOGIES LTD
EAIN	Ethical AI Novelties
LIBRA	Libra AI Technologies
GDPR	General Data Protection Regulation
VPN	Virtual Private Network
EHR	Electronic Health Records
ACID	Atomicity, Consistency, Isolation, Durability
DdoS	Distributed Denial-of-Service
CT	Computed Tomography
MRI	Magnetic Resonance Imaging
IT	Information Technology
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
OIDC	OpenID Connect
UMA	User-Managed Access

1. Introduction

The AERAS project's objective is to establish a robust and adaptable cybersecurity framework tailored to healthcare environments, a sector with unique technical, operational, and regulatory challenges. Deliverable D5.3 aligns with this objective by providing a structured validation of the platform's initial deployment. This deliverable's validation framework is grounded in the principles and Key Performance Indicators' (KPI) defined in D5.2, focusing on critical evaluation dimensions such as system readiness, user familiarity, operational security, and compliance with healthcare-specific cybersecurity protocols. By situating the AERAS platform within a smart hospital environment, D5.3 offers a direct and realistic assessment of its capacity to support hospital staff in recognizing and responding to cybersecurity threats, thereby strengthening organizational resilience. The insights gained from D5.3 will inform platform improvements in functionality, usability, and adaptability, contributing to the AERAS project's overarching aim of enhancing cybersecurity across diverse healthcare settings.

1.1 Role of the Deliverable

Deliverable D5.3, the AERAS Initial Prototype Pilot Validation Report, focusing on the validation of the AERAS cybersecurity platform's deployment within a real-world healthcare environment at University of Patras's (UPAT) and Panepistimiako Geniko Nosokomeio Irakleiou (PAGNI) hospital. The objective of D5.3 is to critically assess the operational efficacy, integration, and user engagement of AERAS's initial prototype, evaluating its ability to address cybersecurity challenges unique to healthcare. This deliverable aims to establish the platform's baseline performance by analyzing technical functionality, adherence to cybersecurity protocols, and the effectiveness of its training programs for end-users in addressing simulated advanced cyber threats.

In advancing the AERAS project's overarching goal to enhance cybersecurity readiness in medical settings, D5.3 documents the initial deployment's outcomes and identifies actionable insights for platform refinement. This report also supports the iterative development of AERAS by documenting user feedback, performance data, and system effectiveness, which will serve as foundational inputs for platform optimization ahead of broader deployment in healthcare systems.

1.2 Relationship to other Deliverables

Deliverable D5.3 occupies a pivotal position within the AERAS project, synthesizing foundational developments from prior work packages while generating critical insights that will inform subsequent stages of platform refinement and evaluation.

This deliverable builds on the architectural and methodological frameworks established in D2.3, which defined the foundational structure and operational principles of the AERAS platform. The architectural insights provided by D2.3 have been instrumental in shaping the integrated components deployed and evaluated in this deliverable. Furthermore, D3.1 (WP3) contributed essential cybersecurity training modules and simulation content, while D4.1 and D4.2 (WP4) introduced advanced monitoring, assessment, and adaptation mechanisms. Together, these

deliverables have provided the technical, functional, and procedural groundwork for the activities undertaken in D5.3.

D5.3 is linked to D5.1, which documented the initial prototype of the integrated AERAS platform, including its architectural components, quality assurance procedures, and technical configuration. The integration work described in D5.1 is applied in D5.3 to deploy and test the prototype within UPAT's hospital environment. This deliverable operationalizes the refined evaluation methodologies and KPIs introduced in D5.2, enabling an assessment of the platform's effectiveness, usability, and cybersecurity impact.

1.3 Structure of the document

This deliverable is systematically structured to provide a comprehensive evaluation of the AERAS platform's initial prototype deployment, focusing on its integration, user training, and initial performance in UPAT's hospital environment. Each section contributes to the iterative validation process and highlights actionable insights for refining the platform:

- Section 2: Pilot Deployment Framework: Provides an in-depth analysis of UPAT's and PAGNI's hospital environment, including its technological and organizational infrastructure. It identifies the specific technical, cybersecurity, and operational requirements necessary for deploying the AERAS platform and details the integration process with existing hospital systems, focusing on data flow and security considerations.
- Section 3: System Readiness, User Training, and Familiarization: Summarizes the training framework established under the Cyber Range Security Assurance (CRSA) model, tailored to enhance cybersecurity awareness and incident response capabilities among hospital staff. This section describes the training materials and delivery methods, as well as the onboarding process for end-users, encompassing demonstrations and practice sessions.
- Section 4: Comprehensive Evaluation and Recommendations for the Initial Prototype Pilot: The evaluation methodology was conducted in two phases. Phase 1 focused on assessing the initial prototype using metrics, usability tests, and feedback mechanisms to evaluate system functionality and user engagement. Phase 2 outlined the methods for evaluating improvements implemented post-Phase 1, using refined KPIs and criteria to emphasize user satisfaction, platform responsiveness, and cybersecurity effectiveness.
  Findings from the initial pilot evaluation were compiled and synthesized to provide key insights into system performance, user feedback on accessibility and usability, and adherence to data protection and cybersecurity compliance standards. Identified technical issues or system defects were categorized by severity, with documented actions taken to address them. Targeted enhancements were proposed to improve platform functionality, usability, and scalability. These include considerations for AERAS's potential deployment in other healthcare settings and a roadmap for further development and testing following D5.3. The recommendations align with project milestones, ensuring a seamless transition to subsequent phases.
- Section 5: Conclusions: Summarizes the primary findings of this deliverable, reflecting on the insights gained from the pilot validation and the contributions of D5.3 to the AERAS

project. This section emphasizes the platform's current impact and potential to advance cybersecurity practices in the healthcare sector.

Each section is designed to build a comprehensive understanding of the AERAS platform's initial validation, guiding the reader from the pilot's preparatory stages through its evaluation outcomes and recommendations for future refinements. This structured approach ensures the deliverable's alignment with the AERAS project's goals while providing actionable insights to inform the platform's development.

2. Pilot Deployment Framework

The AERAS platform is a highly advanced, containerized cybersecurity solution engineered to address the complex needs of healthcare environments. Its modular architecture is built to optimize scalability, reliability, and interoperability, leveraging contemporary technologies such as Kubernetes for orchestration, Keycloak for authentication, and KYPO Cyber Range for simulation environments. These technologies are integrated to enable streamlined management, secure data handling, and dynamic training simulations.

The platform operates on a Kubernetes-orchestrated infrastructure that facilitates the deployment, scaling, and management of its microservices architecture. Kubernetes provides automated resource allocation, container isolation, and load balancing, ensuring consistent performance even under high system utilization. This orchestration enables the platform to dynamically respond to workload demands, such as intensive simulations or simultaneous user access during training sessions. Each containerized component—spanning data processing, training management, and monitoring functions—is isolated, enhancing both security and fault tolerance. Kubernetes also simplifies lifecycle management by automating updates and rollbacks, reducing downtime and ensuring that critical services remain operational.

Access to the platform is secured through Keycloak, an enterprise-grade identity and access management system. Keycloak integrates with the AERAS platform to enforce OpenID Connect and User-Managed Access (UMA) protocols, enabling secure, token-based authentication and granular role-based access control. This ensures that users, whether at UPAT or PAGNI, can securely authenticate and access platform functionalities while maintaining strict separation of privileges. Keycloak's centralized management supports seamless user provisioning, session tracking, and compliance with healthcare-specific regulatory requirements.

The platform's data storage architecture employs a dual-layered system optimized for both structured and unstructured data. PostgreSQL is used to manage transactional data, such as user activity logs and training results, ensuring Atomicity, Consistency, Isolation, Durability (ACID) compliance for reliable data integrity. Concurrently, Elasticsearch is deployed for high-velocity indexing and querying of unstructured data, such as log files and system performance metrics. Data encryption protocols are implemented at both the storage and transmission layers, using advanced cryptographic standards to ensure compliance with General Data Protection Regulation (GDPR) and other data protection regulations. Kubernetes further supports the data infrastructure by orchestrating secure, containerized storage instances, isolating sensitive datasets, and facilitating scalability across distributed nodes.

A critical component of the AERAS platform is the KYPO Cyber Range, a simulation engine designed to create high-fidelity cybersecurity training environments. KYPO integrates with the platform to deliver scenario-driven simulations, allowing users to engage with realistic attack scenarios, including phishing campaigns, malware propagation, and ransomware incidents. The dynamic provisioning of KYPO training environments is managed through Kubernetes, which allocates computational resources in real time to support varying complexity levels of simulations. This ensures optimal performance without overburdening the underlying infrastructure.

Connectivity between the pilot sites at UPAT and PAGNI is established via dedicated VPN channels, ensuring a secure and encrypted communication pipeline. These VPNs facilitate real-time data

exchange and operational synchronization, enabling collaborative training sessions and centralized system management across geographically dispersed locations. The VPN infrastructure is configured to support low-latency communication, critical for maintaining the integrity of live training scenarios and immediate feedback loops. This architecture also ensures that sensitive clinical and operational data remain protected during transmission.

The platform's integration with hospital IT systems at both sites demonstrates its adaptability to varied healthcare infrastructures. By interfacing with Electronic Health Records (EHR) systems, network monitoring tools, and connected medical devices, the AERAS platform enables simulations that replicate real-world operational threats. Kubernetes plays a pivotal role in managing these integrations, orchestrating lightweight, containerized microservices that bridge the platform with existing hospital systems. This design supports interoperability while minimizing disruption to routine hospital operations.

In summary, the AERAS platform's technologically advanced infrastructure, underpinned by Kubernetes, Keycloak, and KYPO, delivers a robust, secure, and scalable solution for cybersecurity in healthcare. Its modular architecture, secure connectivity, and adaptive simulation capabilities ensure that it meets the high demands of healthcare environments while maintaining compliance with stringent regulatory standards. The deployment of the platform across UPAT and PAGNI validates its effectiveness in diverse operational contexts and provides a strong foundation for broader application.

3. System Readiness, User Training and Familiarization

3.1 Objectives of CRSA-driven Training Programs Role of the Deliverable

The CRSA-driven training programs were developed to enhance hospital staff's cybersecurity awareness and response capabilities, addressing the rising cyber threats to healthcare systems. Through carefully constructed questionnaires, the programs evaluated users' preparedness and ability to identify, respond to, and mitigate sophisticated cyberattacks, including phishing emails, ransomware infections, and distributed denial-of-service (DDoS) attacks. These assessments also gauged participants' understanding of compliance with data protection regulations and encouraged reflection on technical and procedural competencies. Insights gained from this process served as a critical preparatory step for deploying the AERAS platform, ensuring end-users were informed about its functionalities and confident in using it to safeguard hospital operations.

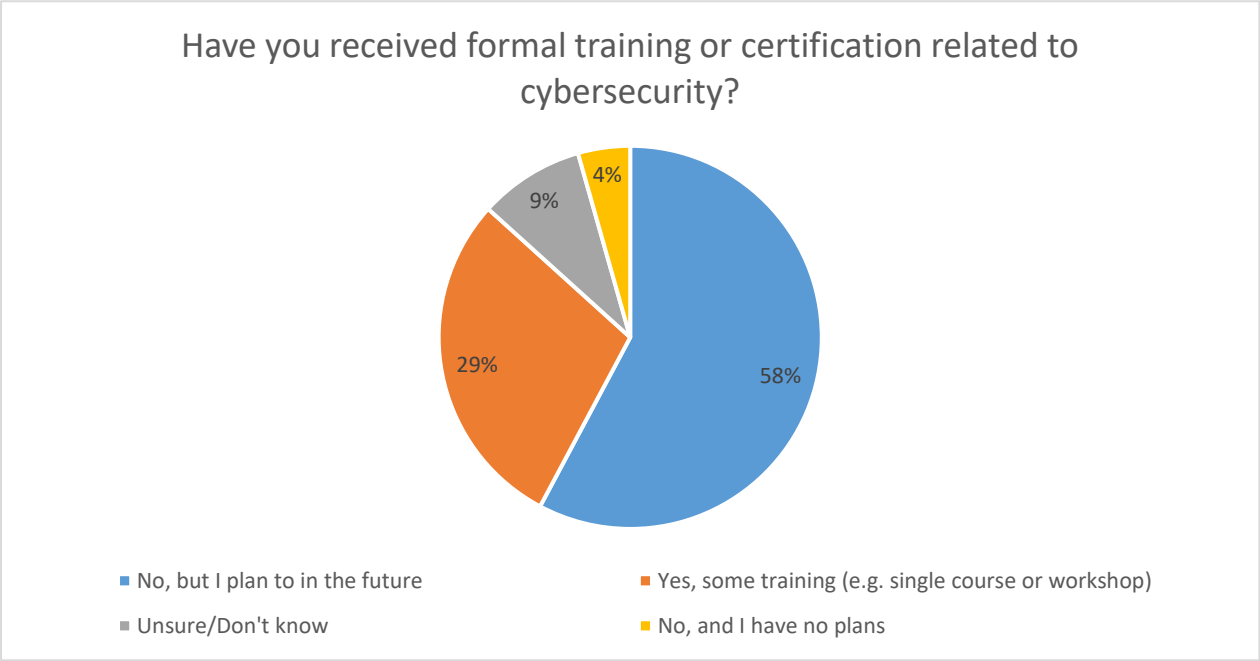

Figure 1: Pie chart of percentage of responses to the question: Have you received formal training or certification related to cybersecurity?

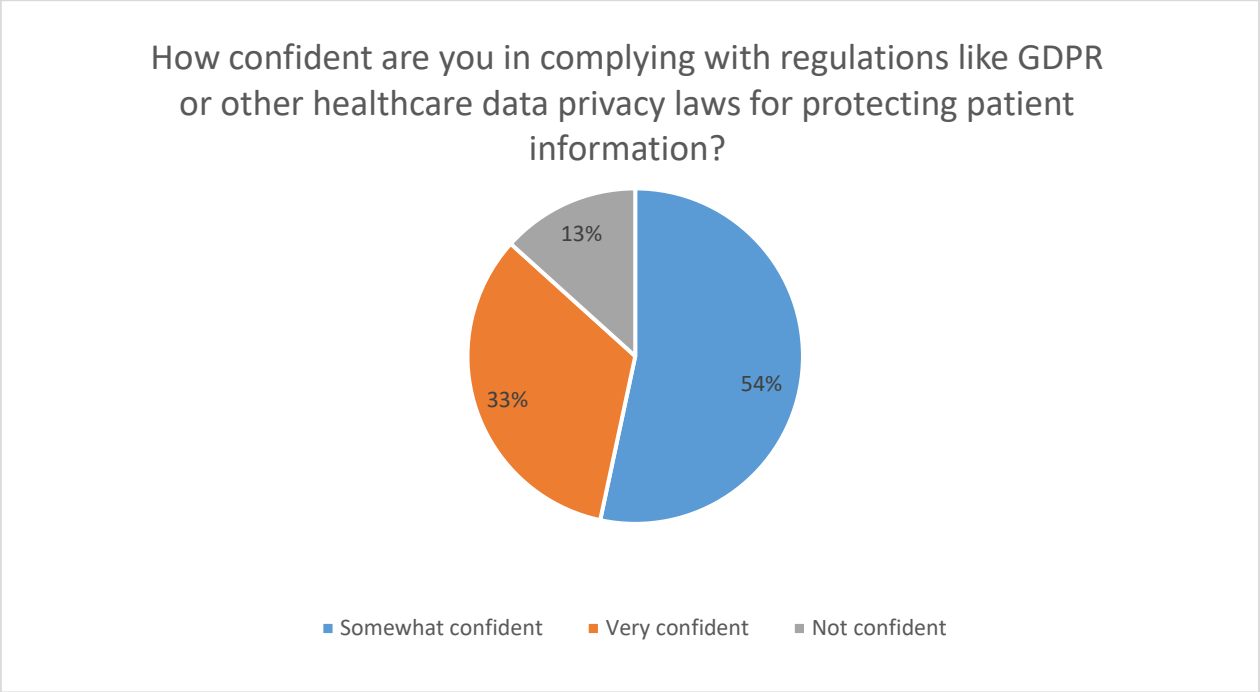

Figure 2: Pie chart of percentage of responses to the question: How confident are you in complying with regulations like GDPR or other healthcare data privacy laws for protecting patient information?

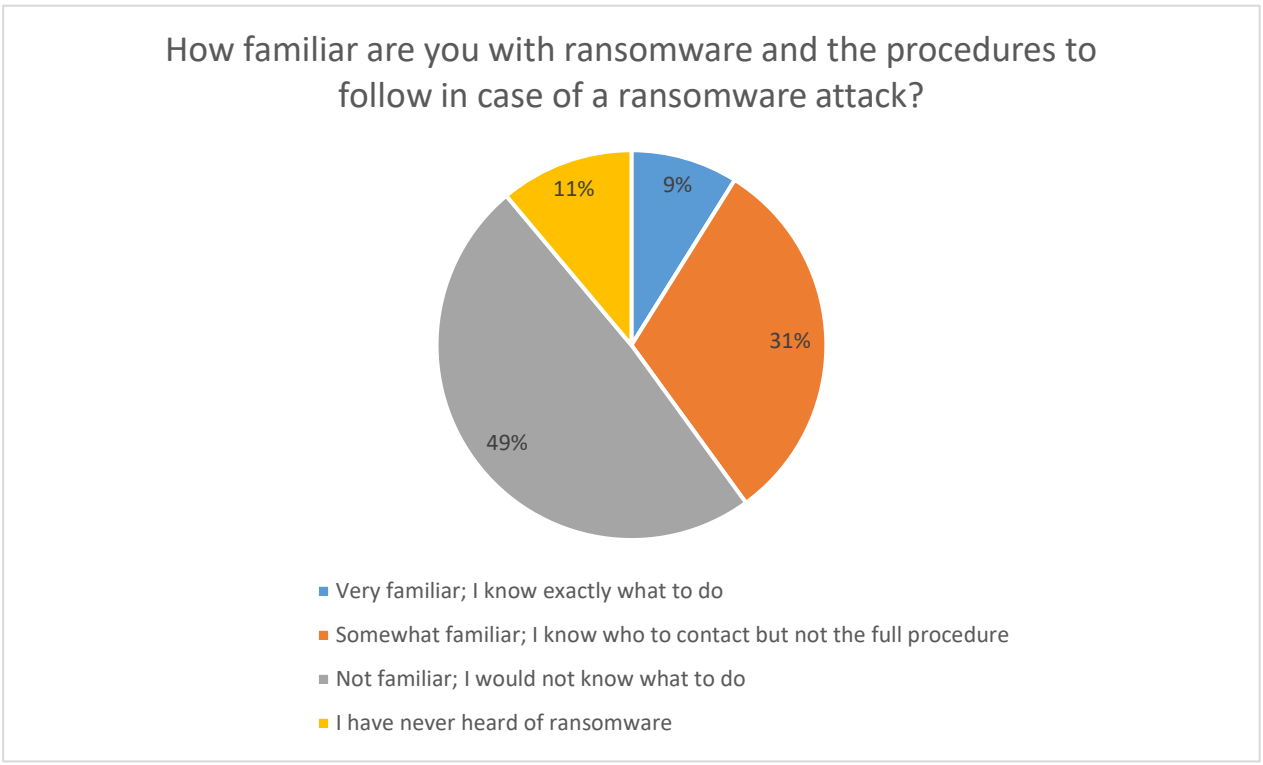

Figure 3: Pie chart of percentage of responses to the question: How familiar are you with ransomware and the procedures to follow in case of a ransomware attack?

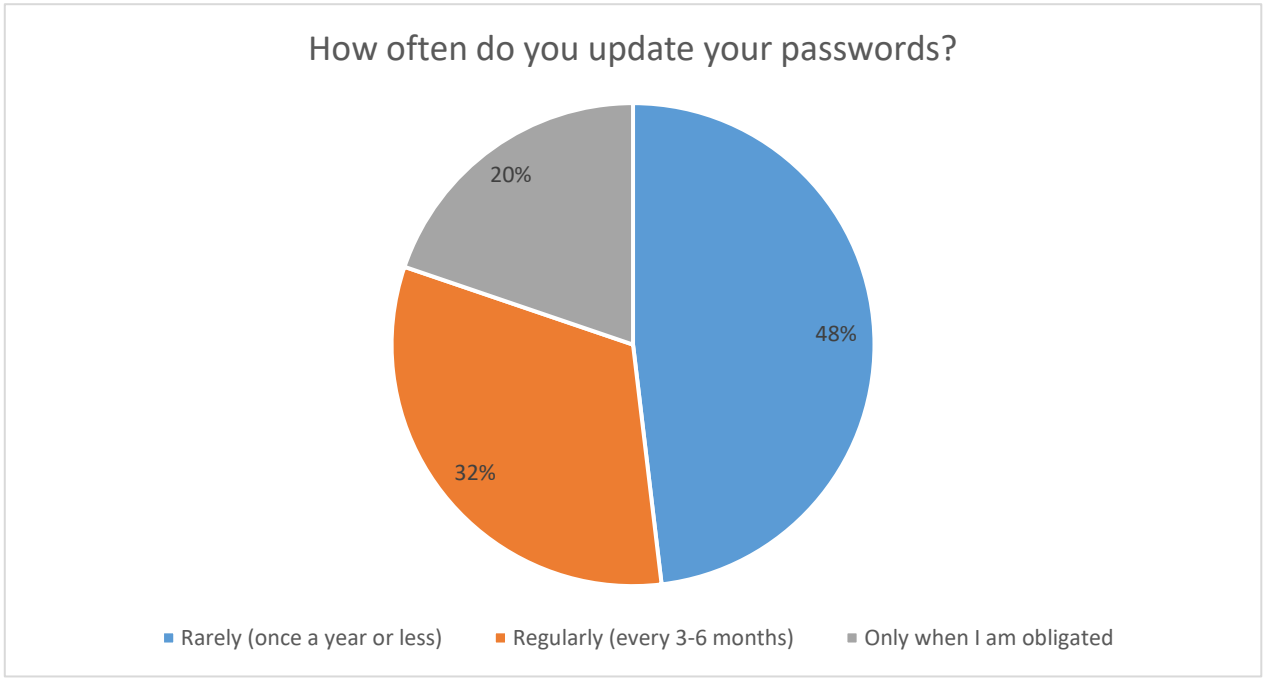

Figure 4: Pie chart of percentage of responses to the question: How often do you update your passwords?

In addition to evaluating technical skills, the programs aimed to foster a culture of cybersecurity awareness within the hospital environment. Many healthcare professionals, particularly those in clinical or administrative roles, may lack familiarity with advanced cyber threats due to the historically limited integration of IT-specific training in their routines. The questionnaires addressed this gap by offering accessible, role-specific content tailored to the diverse responsibilities of hospital staff. This approach ensured that participants across all departments, including clinicians, medical physicists, administrative staff, and IT personnel, could benefit from the assessments.

Based on the survey analysis of cybersecurity practices in healthcare environments, several areas were identified as critical for the CRSA-driven programs. Given that 73.3% of respondents reported encountering phishing attacks, the questionnaires focused on evaluating users' ability to recognize phishing emails, avoid malicious links, and follow proper reporting procedures. Additionally, 35.6% of respondents reported malware infections, while 48.9% indicated that there were no restrictions on external device use. Consequently, the assessments emphasized the importance of securely handling USB devices and recognizing ransomware threats. To address potential service disruptions affecting 24/7 healthcare operations, the questionnaires included items on recognizing signs of DDoS attacks and understanding mitigation strategies. Furthermore, identity spoofing was identified as a concern, particularly since 33.3% of respondents were unsure of incident reporting procedures. Therefore, the assessments included methods for verifying email authenticity to combat identity spoofing.

The questionnaires incorporated scenario-based queries to enhance practical engagement, an approach recommended by 40% of respondents. Another key objective of the programs was to ensure alignment between the capabilities of the AERAS platform and the hospital's operational needs. Users were introduced to critical features such as the threat monitoring dashboard, incident response tools, and reporting mechanisms, enabling them to understand the platform's functionalities in real-world contexts.

Furthermore, the programs sought to assess and enhance user confidence in addressing cyber threats. A vital component of this objective was the use of scenario-based questions, which required participants to apply their knowledge in simulated cyberattack contexts. These scenarios were designed to replicate the complexities of actual threats, encouraging users to adopt proactive strategies while understanding the AERAS platform's role in supporting incident resolution.

The CRSA-driven programs were also instrumental in generating user feedback to inform iterative refinements of the AERAS platform. The questionnaires provided opportunities for participants to share their experiences and offer input on the platform's usability, effectiveness, and relevance to their roles. This feedback was collected and analyzed to ensure that the platform's development remained user-centered and aligned with operational realities.

3.2 Training Materials and Delivery Methods

The questionnaire included in the annex was a key tool for evaluating and driving the implementation of the AERAS platform and its associated CRSA-driven training programs. Its primary purpose was to collect structured feedback from hospital staff, offering both quantitative and qualitative insights. This feedback assessed the effectiveness of training, the usability of the platform, and the preparedness of participants in addressing cybersecurity threats. By gathering direct user input, the questionnaire will provide evidence of the platform's alignment with the operational needs of healthcare professionals in a real-world setting.

The content was divided into sections to ensure a comprehensive assessment. These sections included demographic information, training evaluation, platform usability, preparedness for cyber threats, and feedback. Each section was designed to capture data relevant to the user experience, allowing trends to emerge across roles, levels of experience, and interaction with hospital IT systems.

The demographic section provided context by gathering information on participants' roles, departments, and prior cybersecurity experience. This data enabled the analysis of feedback based on the professional background of respondents. The training evaluation section assessed the relevance, clarity, and delivery of the CRSA-based modules must have to be included in the pilot phase. It included questions about the realism of the scenarios and the effectiveness of the training in addressing cybersecurity risks specific to healthcare environments.

After the pilot execution, the trainees will be asked to fill additional questionnaire in order to evaluate the quality of the AERAS solution. First, a platform usability section to examine the interface and functionality of the AERAS platform as experienced during the training. Participants will be asked about the intuitiveness of the system, ease of navigation, and accessibility of features. These questions will identify strengths and areas needing improvement, particularly in user interaction with dashboards, alerts, and incident management tools.

Then, trainees will supply a short report on confidence levels they have had in responding to cyber threats proposed in the training. It will measure how well participants felt equipped to apply the knowledge and skills gained during the training. Scenario-based questions will explore their readiness to handle specific incidents, such as phishing attacks or malware detection.

Finally, participants will provide open-ended feedback. This qualitative component added depth to the evaluation, capturing insights that quantitative data could not reveal. Respondents can elaborate on challenges, highlighted specific platform features, and offered suggestions for improvement. These responses will be instrumental in identifying nuanced issues and guiding targeted enhancements.

IT is important to note that the questionnaire included in the annex was designed with a mixed-methods approach, combining quantitative and qualitative data collection. Likert-scale questions enabled statistical analysis of satisfaction, training impact, and usability. Open-ended questions enriched the findings with detailed user experiences and suggestions. This balance ensured both rigor and depth in the evaluation.

The implementation of the questionnaire followed strict ethical standards. It was administered immediately after the training sessions to ensure accurate recall. Responses were anonymized to encourage honest feedback. Informed consent was obtained from all participants, and data protection guidelines were strictly followed.

The same approach will be followed for the post-training questionnaire. The data collected through the questionnaire will be central to the pilot evaluation. They will evaluate the effectiveness of the CRSA/CRST-based training and the usability of the AERAS platform. The findings will highlight areas of success and identified opportunities for improvement. These insights will form a foundation for iterative refinement, ensuring the platform's alignment with the needs of healthcare professionals and the objectives of the AERAS project.

By focusing on the feedback provided in the questionnaires, it will be ensured that the platform's development was informed by practical insights, making it more effective and user-centered. It will provide a structured means of assessing how well the AERAS platform addressed real-world cybersecurity challenges. The questionnaire ensured that the platform's development was informed by practical feedback, making it more effective and user- centred.

3.3 Structured Onboarding Process

The training process for the AERAS platform pilots was designed to ensure participants gained a thorough understanding of the platform's capabilities while providing valuable feedback for its refinement. This structured approach combined theoretical orientation, hands-on practice, and systematic feedback collection to prepare participants for effective engagement with the platform and generate actionable insights for its evaluation.

A critical aspect of this process was the questionnaire, administered before the training sessions. The primary purpose of this questionnaire was to identify the participants' training needs and inform the development of targeted training modules. It was emphasized that this tool served solely as a preparatory measure for identifying training concepts, rather than as an evaluative metric for the platform's capabilities.

The training began with an orientation session introducing participants to the AERAS platform's key features and functionalities. Guided demonstrations highlighted the platform's relevance to the unique cybersecurity challenges in healthcare settings. Participants were shown how to navigate the threat monitoring dashboard, incident reporting tools, and compliance tracking modules. These

demonstrations were tailored to various levels of technical expertise, ensuring accessibility for both IT personnel and clinical staff. Real-time examples illustrated how the platform integrates with hospital workflows and mitigates cyber threats.

Building on this foundation, participants engaged in interactive training sessions conducted in controlled environments that simulated real-world cybersecurity scenarios. Exercises included identifying and responding to phishing attacks, isolating ransomware threats, and managing unauthorized access attempts. Trainers provided continuous support, answering questions and offering personalized feedback. Tiered challenges accommodated both technical and non-technical staff, enabling effective skill development across all participants.

This integrated approach—combining pre-training preparation and hands-on learning—ensured that participants were equipped to utilize the platform effectively. By aligning the training process with the operational realities of the pilot sites, the AERAS training methodology validated the platform's relevance and usability while supporting its continuous refinement.

4. Comprehensive Evaluation and Recommendations for the Initial Prototype Pilot

4.1 Overview of Evaluation Phases

The evaluation process for the AERAS platform was structured into two cohesive and interrelated phases: Phase 1, the Initial Prototype Evaluation, and Phase 2, the Final Prototype Evaluation. These phases were systematically designed to assess the platform's performance and ensure its alignment with the broader objectives of the AERAS project, particularly in addressing cybersecurity challenges in healthcare settings.

Phase 1 established the groundwork for the platform's deployment, emphasizing its initial implementation and integration within the operational frameworks of UPAT and PAGNI hospitals. This stage focused on baseline evaluations of the platform's technical capabilities, user interface, and compatibility with existing hospital workflows. It also examined how effectively the platform addressed cybersecurity vulnerabilities in a real-world environment. Feedback collected during this phase highlighted user experiences and operational gaps, offering essential insights for the platform's iterative refinement. Training activities during Phase 1 were informed by detailed findings from structured questionnaires, enabling the identification of specific areas where each hospital site faced unique cybersecurity challenges.

Phase 2 built on the outcomes and lessons learned during Phase 1, introducing targeted enhancements to the platform. These adjustments were specifically designed to address the identified deficiencies, improve user engagement, and optimize operational efficiency. This phase focused on validating the platform's upgraded features, with a particular emphasis on user satisfaction, practical functionality, and the platform's ability to mitigate cybersecurity threats effectively. Training programs during Phase 2 incorporated advanced scenario-based exercises, reflecting the platform's improved capabilities and addressing the evolving needs of participants. Structured evaluation tools, coupled with performance metrics, provided robust evidence of the platform's enhanced usability and effectiveness.

Both phases of the evaluation were grounded in thorough preparatory activities. These included system readiness tests to ensure the platform's seamless integration with hospital systems and comprehensive user familiarization sessions to equip participants with the necessary skills to engage with the platform. By adopting this phased approach, the evaluation process ensured that the platform's development remained iterative, user-focused, and aligned with the strategic priorities of the AERAS project.

4.2 Key Findings on System Performance

The participant pool featured a diverse range of roles, with physicians forming the largest group, followed by a substantial representation of medical physicists. Smaller groups included IT professionals and radiographers, contributing specialized insights on the platform's usability and performance. The respondents were predominantly experienced professionals with over a decade in their roles, while a smaller proportion brought perspectives from early-career positions, offering a blend of seasoned expertise and fresh viewpoints.

General cybersecurity awareness levels were reported as moderate by a significant portion of respondents, with a smaller contingent displaying high awareness. However, a notable segment indicated low levels of awareness, underscoring gaps in knowledge that could compromise organizational security. Formal training in cybersecurity was not widely prevalent, with 57.8% of participants indicating that they had not undergone any formal cybersecurity training, highlighting an urgent need for structured programs.

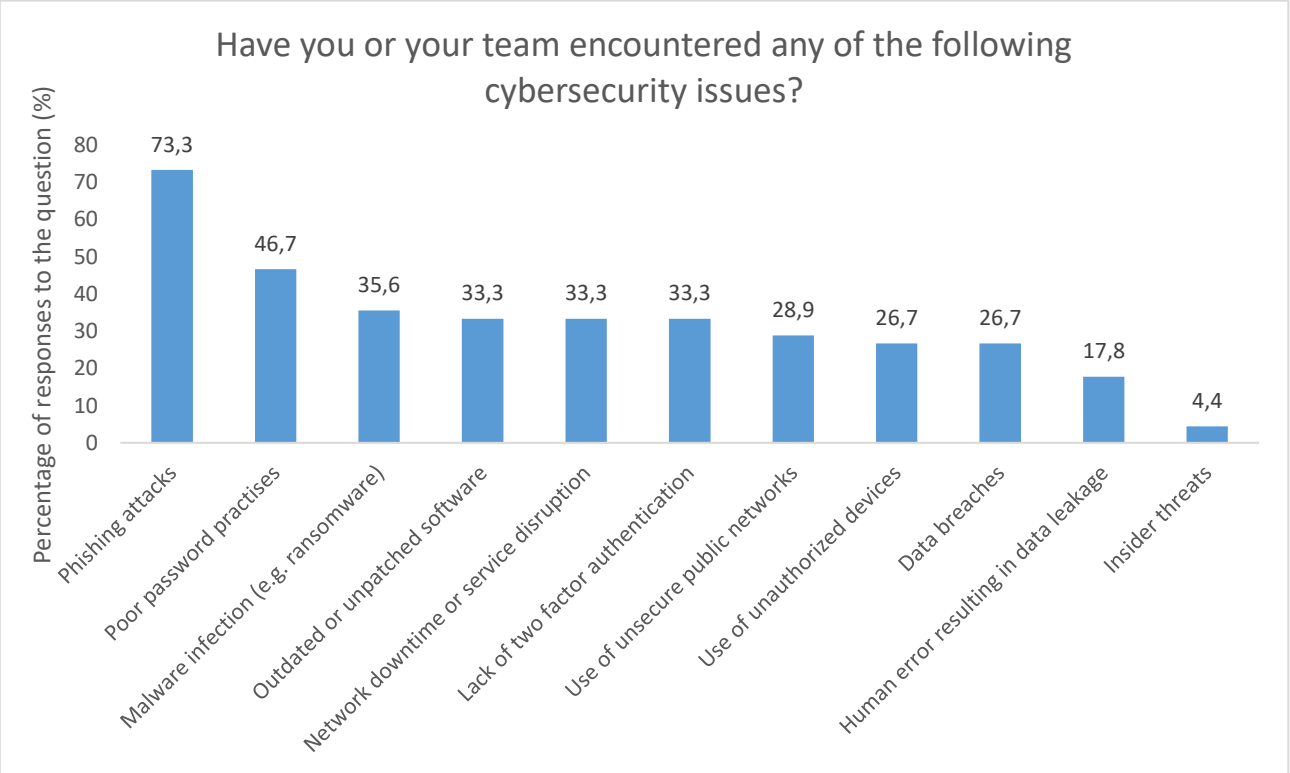

Figure 3: Chart of percentage of responses to the question: Have you or your team encountered any of the following cybersecurity issues?

Phishing attacks emerged as the most frequently encountered cybersecurity threat, affecting 73.3% of respondents. Additional challenges identified included poor password practices (46.7%) and malware infections (35.6%). Medical device security also revealed significant gaps, with only 15.6% of respondents aware of established cybersecurity protocols for these devices, indicating a clear need for targeted training and policy development in this area.

Incident reporting practices presented another challenge; while 66.7% of participants knew the appropriate channels for reporting a cyberattack, 33.3% were unsure, emphasizing the need for standardized reporting procedures across the organization. Remote work practices further

highlighted vulnerabilities, as 6.7% of respondents admitted to using personal email for work purposes, pointing to a need for clear and robust remote work guidelines to mitigate these risks.

These findings reinforce the necessity of implementing targeted training on phishing, ransomware, and DDoS attacks, as well as improving incident reporting mechanisms and medical device security protocols.

Operationally, phishing attacks continued to pose the greatest threat. Inconsistent password practices and infrequent software updates contributed to system vulnerabilities. While some participants adhered to secure password protocols, others did not consistently follow best practices, underscoring the pressing need for stricter password policies and user education.

Medical imaging devices, including Magnetic Resonance Imaging (MRI) and Computed Tomography (CT) systems, were identified as critical points of within the healthcare ecosystem. Many respondents highlighted concerns such as outdated or unpatched software and the use of unauthorized devices, which pose significant risks to data security and operational workflows. Confidence in managing cybersecurity risks related to these devices varied widely, with many users expressing a lack of assurance, reinforcing the need for specialized training and technical support.

Remote work practices also revealed challenges. While a large number of respondents adhered to secure protocols when accessing hospital systems remotely, a smaller yet notable group reported using personal email or file-sharing platforms for work purposes, exposing potential vulnerabilities. These behaviors emphasize the necessity of implementing robust governance measures and establishing clear remote work guidelines.

4.3 Adherence to Cybersecurity Compliance Requirements

The evaluation revealed strengths and gaps in adherence to cybersecurity compliance requirements. IT professionals demonstrated a strong understanding of frameworks such as GDPR, but awareness levels among clinical staff were notably lower. A significant share of participants lacked familiarity with organizational protocols for safeguarding medical devices, suggesting that cross-disciplinary training is necessary to bridge knowledge gaps.

Incident reporting processes varied among participants. While many understood the appropriate channels for reporting cybersecurity incidents, a subset of respondents expressed uncertainty, which could delay timely responses and mitigation efforts. This inconsistency underscores the importance of standardized reporting procedures and effective communication across all roles.

The platform exhibited robust compliance features, such as integrated antivirus solutions and encryption protocols. However, the lack of multi-factor authentication (MFA) for many users represents a critical vulnerability, leaving systems susceptible to unauthorized access. Additionally, proactive measures like simulated phishing exercises were employed by only a small fraction of organizations, underscoring the need for broader adoption of such practices to strengthen preparedness.

Training modules on GDPR and data privacy addressed some compliance aspects but were perceived as insufficient by participants in non-technical roles. More tailored training on incident response, secure data handling, and regulatory requirements is essential to foster comprehensive compliance across the workforce.

4.4 Identified Technical Issues and Defect Resolution

Several technical challenges and usability concerns impacting the platform's effectiveness were identified during the evaluation. Many participants highlighted issues with outdated or unpatched software on medical devices, which compromised both security and operational efficiency. Unauthorized use of external devices, such as USB drives, was another recurring concern, increasing the risk of data breaches and malware infections.

Non-technical staff, including physicians and radiographers, reported greater difficulty navigating the platform compared to their technical counterparts. These usability challenges underline the need for enhancements to the user interface and more comprehensive onboarding processes to ensure all users can interact effectively with the platform.

Data backup practices were inconsistent across respondents. While some adhered to systematic backup schedules, others reported irregular practices, creating potential risks for data loss in the event of a cyberattack. Incident reporting workflows also emerged as a significant pain point, with some respondents describing them as cumbersome or unclear, further emphasizing the need for streamlined processes.

Despite these challenges, the platform demonstrated notable strengths in providing real-time threat alerts and actionable insights. Many participants recognized these capabilities as critical for improving situational awareness and organizational resilience. Addressing the technical and usability challenges identified will be key to unlocking the platform's full potential.

Proposed solutions to address these issues include:

- Implementing automated software updates to ensure security and operational continuity.
- Enforcing MFA requirements for all users accessing sensitive systems and data.
- Redesigning the platform's user interface to enhance accessibility for less technical users.
- Establishing clearer, more efficient incident reporting workflows and escalation protocols.

4.5 Platform Improvements Based on User Feedback

Feedback from users during the pilot evaluation emphasized the need for refinements to optimize the platform's usability, enhance its training integration, and address technical challenges. Usability improvements should focus on creating a more intuitive interface, particularly for non-technical users, by incorporating simplified workflows and integrated guidance tools. Advanced features such as custom reporting, while powerful, require clearer instructional support to ensure broader adoption across diverse user groups.

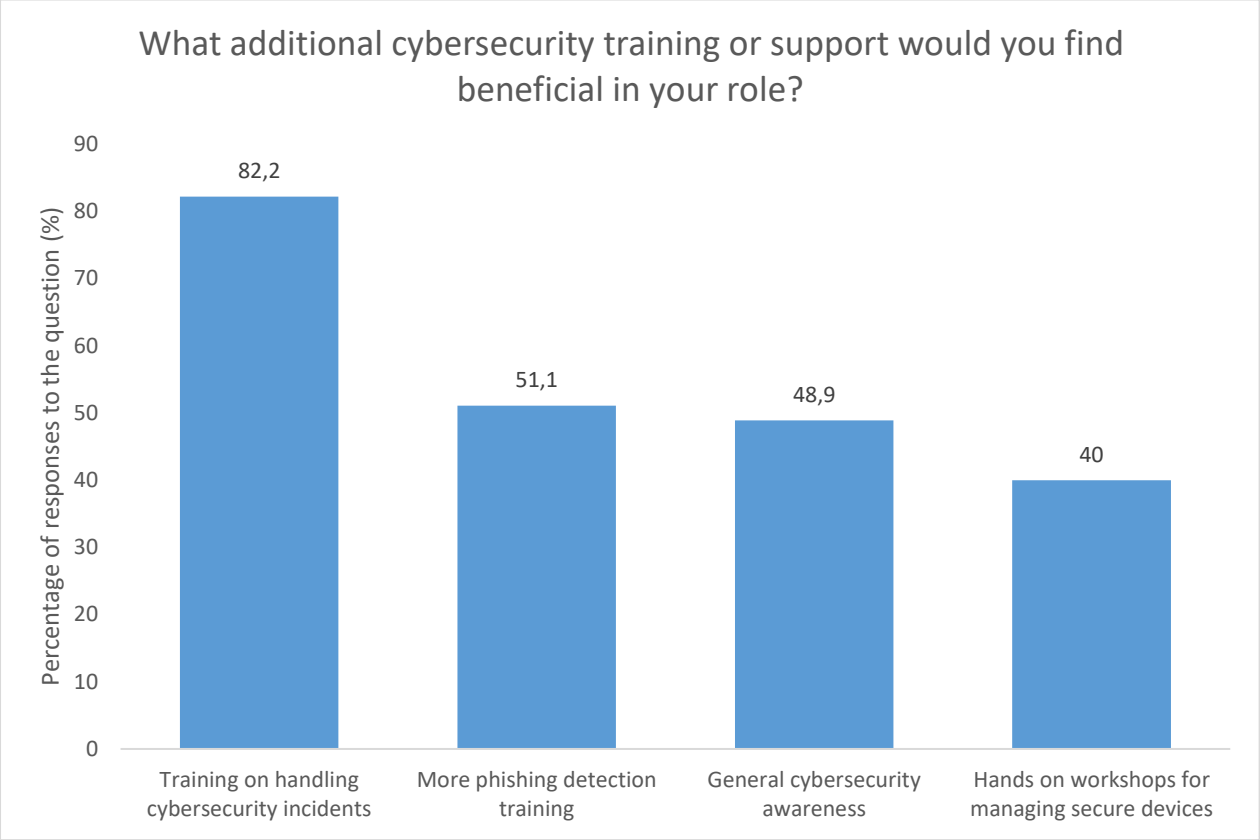

Figure 6: Chart of percentage of responses to the question: What additional cybersecurity training or support would you find beneficial in your role?

To address disparities in training outcomes, the platform should integrate tailored and role-specific training modules. These modules should include interactive tutorials and scenario-based exercises designed to align with the varying expertise levels of users, ranging from clinicians to IT personnel. Enhanced simulation exercises that offer tiered levels of complexity will ensure that users with minimal technical background can engage effectively with the platform. Survey results highlight additional areas for targeted training. Comprehensive modules on recognizing and reporting phishing attacks are necessary to address the 73.3% of respondents who reported encountering phishing threats. Training on ransomware prevention, including safe use of external devices and identifying malware infections, should be prioritized, given that 48.9% of users reported unrestricted use of such devices. DDoS attack preparedness must be enhanced with training focused on mitigating service disruptions, ensuring continuous 24/7 operations. Clear and standardized incident reporting procedures should be developed to address the 33.3% of respondents who were unsure about the appropriate contacts during a cyberattack. Furthermore, protocols and training

on securing medical imaging devices are essential, considering only 15.6% of users were aware of existing security policies for these devices. These training modules should incorporate hands-on workshops and simulated exercises to increase engagement and practical understanding.

Issues with the platform's threat notification system, such as duplicate alerts, need resolution through refined synchronization mechanisms and improved prioritization algorithms. Ensuring that alerts are contextually relevant and actionable will reduce confusion and increase user confidence in responding to threats. Additionally, the integration of medical imaging devices into the platform's monitoring infrastructure is critical. Many of these devices operate on outdated software, representing a significant cybersecurity vulnerability. Automated update protocols and enhanced encryption measures must be implemented to mitigate risks associated with these critical systems.

4.6 Scalability and Replication Potential

The scalability of the AERAS platform is a vital factor for its broader deployment across healthcare settings. The modular architecture of the platform supports its adaptability to different operational environments, including small clinics, large hospitals, and multi-site healthcare systems. However, deployment in resource-constrained settings requires careful consideration of infrastructure limitations. Cloud-based deployment options with lightweight client interfaces can enable accessibility in environments with minimal hardware resources.

Ensuring interoperability with various healthcare IT systems, including EHRs and telemedicine platforms, is essential for seamless integration.

To address regional variations in regulatory and operational practices, the platform must be customized to comply with local cybersecurity frameworks and data protection laws. This adaptability will ensure broader acceptance while maintaining the platform's effectiveness.

4.7 Key Milestones for Further Development

User feedback must guide immediate refinements to improve the platform's interface, notification system, and training modules. These efforts should be complemented by the integration of automated update protocols for legacy systems, addressing vulnerabilities in medical imaging devices.

Mid-term goals include scaling the platform for broader deployment by developing adaptable configurations for varied healthcare settings. This will involve enhancing interoperability with additional standardized data exchange protocols and expanding training materials to include culturally adapted and multilingual content. Collaboration with institutions in diverse regions will validate the platform's adaptability to different operational needs.

Long-term development will focus on conducting multi-site trials to test the platform's scalability and robustness in real-world scenarios. These trials will provide critical insights into its effectiveness across a range of healthcare systems, supporting its final validation. Regulatory compliance with international cybersecurity and data protection standards will also be finalized during this phase, ensuring readiness for commercialization or institutional adoption.

5. Conclusions

The pilot evaluation of the AERAS platform, documented in this deliverable, represents a critical milestone in validating its capacity to enhance cybersecurity resilience within healthcare environments. By deploying the platform in UPAT's and PAGNI's smart hospital and engaging users in comprehensive training and testing, this report consolidates insights into the platform's functionality, user engagement, and alignment with organizational needs. This section reflects on the primary insights derived from the evaluation and situates the findings within the broader objectives of the AERAS project.

5.1 Primary Insights from Pilot Evaluation

The pilot evaluation provided significant insights into the platform's strengths, limitations, and potential for broader application. Key takeaways demonstrate that the AERAS platform is well-equipped to address critical cybersecurity challenges, including threat detection, user training, and regulatory compliance. The system's high accuracy in identifying and responding to simulated phishing and ransomware scenarios confirms its operational effectiveness in mitigating real-world threats. The integration of automated response mechanisms further supports its ability to streamline incident resolution, enhancing overall organizational readiness.

The evaluation highlighted that phishing attacks remain a pervasive cybersecurity threat within healthcare environments. This finding underscores the need for targeted training to help staff recognize and respond to phishing attempts effectively. Additionally, the lack of formal cybersecurity education among many users points to an urgent need for structured training programs to improve awareness and response capabilities. The absence of clear policies on external device usage has also revealed vulnerabilities that need to be addressed through stricter guidelines and protocols to prevent malware infections and security breaches.

Knowledge gaps in incident reporting procedures were identified, emphasizing the importance of clearer protocols and more effective communication channels to ensure timely and efficient responses to cybersecurity incidents. The evaluation further highlighted the need for specialized training and stricter policies to protect medical devices, which are critical components of hospital operations. Discrepancies in cybersecurity awareness and preparedness between technical and clinical staff underscore the importance of developing training initiatives tailored to the needs of different user groups.

The pilot also confirmed that the platform aligns with regulatory standards, such as GDPR, though ongoing education is necessary to ensure consistent compliance across all roles. These insights collectively validate the platform's readiness for further refinement and broader deployment, ensuring that it remains adaptable to the evolving cybersecurity landscape in healthcare.

5.2 Contribution of D5.3 to AERAS Goals

This deliverable significantly advances the strategic objectives of the AERAS project, contributing to its overarching aim of creating robust and adaptable cybersecurity solutions for healthcare systems. By conducting a rigorous pilot evaluation, D5.3 serves as a bridge between the development of the platform and its real-world application, ensuring that the system is both functional and user-centric.

The insights gained from this deliverable directly inform the iterative development of the AERAS platform, ensuring that its features are refined to meet the complex demands of healthcare environments. The pilot's findings have identified critical areas for improvement, including the need for stricter policies on external device usage, targeted training to address phishing threats, and clearer protocols for incident reporting. Enhancing training materials and addressing these vulnerabilities will ensure that the platform evolves effectively in response to user feedback and emerging cybersecurity challenges.

D5.3 establishes a foundation for future evaluations by providing a comprehensive assessment of the platform's initial prototype. The methodologies, performance indicators, and user feedback documented in this deliverable will guide the final validation stages, ensuring that the platform is scalable and adaptable to diverse healthcare settings. Furthermore, this deliverable reinforces the project's commitment to fostering a culture of cybersecurity awareness and preparedness within healthcare institutions, positioning the platform as an essential tool for safeguarding patient data and clinical operations.

In conclusion, this deliverable not only validates the platform's current capabilities but also outlines a clear path for its continued development and deployment. By addressing the insights and recommendations presented in this report, the AERAS project moves closer to transforming cybersecurity practices in the healthcare sector, ensuring a safer and more resilient future for medical systems worldwide.

6. Annex A: AERAS Cybersecurity Questionnaire

SECTION 1: GENERAL INFORMATION

1. Your Role in the Organization

a) Executive Management
b) Administrative staff
c) IT/Cybersecurity Professional
d) Operational Technology (OT) Professional
e) Physician
f) Medical Physicist
g) Nurse
h) Other (Please specify)

2. How many years have you been working in your current role?

a) Less than a year
b) 1-3 years
c) 4-6 years
d) 7-10 years
e) More than 10 years

3. What is your highest level of education?

a) High school diploma
b) Associate's degree
c) Bachelor's degree
d) Master's degree
e) Ph.D./Doctoral degree
f) Other (Please specify)

4. Have you received formal training or certification related to cybersecurity?

a) Yes, extensive training (multiple courses or certifications)
b) Yes, some training (e.g., single course or workshop)
c) No, but I plan to in the future
d) No, and I have no plans to
e) Unsure/Don't know

5. How comfortable are you using new technology or digital tools in your job?

a) Very comfortable
b) Somewhat comfortable
c) Neutral
d) Somewhat uncomfortable
e) Very uncomfortable

6. Do you have any responsibilities related to managing or overseeing cybersecurity protocols?

a) Yes, I am directly involved in managing cybersecurity
b) Yes, I am involved but only occasionally
c) No, but I am aware of cybersecurity protocols
d) No, I do not have any involvement

7. How familiar are you with the concept of a "Smart Hospital" and its technological infrastructure?

a) Very familiar
b) Somewhat familiar
c) Neutral
d) Not very familiar
e) I have not heard of it

8. How would you assess your general level of cybersecurity awareness?

a) Very high
b) High
c) Moderate
d) Low
e) Very low

SECTION 2: CYBERSECURITY PRACTICES

9. How often does your organization update you on new cybersecurity threats and safety practices?

a) Every month
b) Every six months
c) Every year
d) Every two years
e) More than two years
f) Unsure/Don't know

10. How would you rate your organization's current cybersecurity posture?

a) Very advanced
b) Advanced
c) Moderate
d) Basic
e) Unsure/Don't know

11. Does your organization restrict the use of external devices (e.g., USB drives, personal smartphones) on work devices?

a) Yes
b) No
c) Unsure/Don't know

12. Does your organization use anti-virus or anti malware software on work devices?

a) Yes
b) No
c) Unsure/Don't know

13. Has your organization ever conducted a simulated phishing exercise to test employee awareness?

a) Yes
b) No
c) Unsure/Don't know

SECTION 3: CYBERSECURITY CHALLENGES

14. Have you or your team encountered any of the following cybersecurity issues? (Select all that apply)

a) Phishing attacks
b) Malware infections (e.g., ransomware)
c) Insider threats
d) Data breaches
e) Outdated or unpatched software
f) Network downtime or service disruption
g) Use of unauthorized devices
h) Poor password practices
i) Use of unsecured public networks
j) Lack of two factor authentication
k) Human error resulting in data leakage
l) Other (Please specify)

15. If you have encountered phishing attacks, how frequently do you receive phishing emails?

a) Daily
b) Weekly
c) Monthly
d) Rarely
e) Never

16. In the case of phishing, do you feel confident identifying and reporting suspicious emails?

a) Yes, I feel confident
b) Somewhat, but I could use more training
c) No, I find it difficult to identify phishing attempts

17. How often do your medical imaging devices (e.g., PET/CT, CT, MRI, Ultrasound) receive software or firmware updates to address potential cybersecurity vulnerabilities?

a) Regularly (every few months)
b) Occasionally (once a year)
c) Rarely
d) Never
e) Unsure

18. How would you describe the ease of reporting a cybersecurity issue (e.g., phishing or malware) within your organization?

a) Very easy
b) Somewhat easy
c) Difficult
d) Unsure how to report
e) I have never needed to report an issue

19. Have you or your team experienced any cybersecurity incidents that have directly impacted the operation of medical imaging devices (e.g., PET/CT, CT, MRI, Ultrasound)?

a) Yes
b) No
c) Unsure

20. Do you feel that patient data security is adequately addressed during the use of medical imaging devices (e.g., PET/CT, CT, MRI, Ultrasound)?

a) Yes, I feel confident
b) Somewhat, but there are gaps
c) No, there are significant vulnerabilities
d) Unsure/Don't know

21. What specific cybersecurity tools or procedures would you suggest be implemented or improved in your hospital's medical imaging devices (e.g., PET/CT, CT, MRI, Ultrasound)? (Select all that apply)

a) Advanced encryption
b) Two-factor authentication
c) Regular phishing simulations
d) Enhanced employee cybersecurity training
e) Restriction on the use of external devices
f) Automated software updates
g) Other (Please specify)

22. How confident are you in handling cybersecurity risks across various medical imaging devices (e.g., PET/CT, CT, MRI, Ultrasound)?

a) Very confident
b) Somewhat confident
c) Not confident
d) Unsure

23. How often do you update your passwords?
a) Regularly (every 3-6 months)
b) Rarely (once a year or less)
c) Only when I am obligated

24. Do you use unique passwords for different systems or applications (e.g., hospital systems, personal accounts)?
a) Always
b) Sometimes
c) Never

25. Does your organization require regular password changes for work-related accounts and systems?
a) Yes
b) No
c) Unsure/Don't know

26. How confident are you in complying with regulations like GDPR or other healthcare data privacy laws for protecting patient information?
a) Very confident
b) Somewhat confident
c) Not confident

27. Does your organization provide regular training on complying with GDPR or other healthcare data privacy regulations?
a) Yes, training is provided regularly (annually or more often)
b) Yes, but training is infrequent
c) No, there is no formal training
d) Unsure

28. Do you understand the hospital's policies on handling and sharing patient data?
a) Yes, very clear
b) Somewhat clear
c) No, I am unsure

29. Do you regularly lock or log out of your workstation when stepping away?
a) Always
b) Sometimes
c) Never

30. Do you use hospital-approved devices to access patient information or hospital systems?
a) Yes, always
b) Sometimes, I use personal devices
c) No, I primarily use personal devices

31. Are you aware of the risks associated with connecting personal devices to hospital networks?
a) Yes, very aware
b) Somewhat aware
c) Not aware

32. Do you know who to report to if you experience or suspect a cyberattack (e.g., ransomware, data breach)?
a) Yes
b) No

33. How quickly would you report an incident such as a suspected data breach or phishing email?
a) Immediately
b) Within a few hours
c) I'm unsure how or when to report

34. Are you aware of the risks associated with using public Wi-Fi networks for work-related activities?
a) Yes
b) No
c) Unsure/Don't know

35. How often do you back-up critical data?
a) After any change
b) Once a month
c) Every six months or more
d) Never

36. How do you verify the identity of someone requesting access to sensitive information or systems?
a) I verify their credentials through the hospital's system
b) I rely on verbal or written confirmation
c) I assume they have access if they ask
d) I don't verify

37. What would you do if you received an email from a familiar colleague asking for confidential information, but the request seems unusual?
a) Send the information without hesitation
b) Double-check the request in person or through another communication channel
c) Ignore the email
d) Delete the email immediately

38. How do you handle sensitive information (e.g., patient data) when working remotely?
a) I use secure hospital-approved systems (e.g., VPN, encrypted channels)
b) I send data over personal email or file-sharing platforms
c) I don't access sensitive data remotely
d) I'm unsure how to handle sensitive data remotely

39. How familiar are you with ransomware and the procedures to follow in case of a ransomware attack?
a) Very familiar; I know exactly what to do
b) Somewhat familiar; I know who to contact but not the full procedure
c) Not familiar; I would not know what to do
d) I have never heard of ransomware

40. Do you use personal cloud services (e.g., Google Drive, Dropbox) to store or share hospital-related documents?
a) Yes, regularly
b) Occasionally
c) Never
d) I'm not sure if it's allowed

41. How would you rate your understanding of the hospital's cybersecurity policies?
a) Very clear, I know and follow them closely
b) Somewhat clear, I follow most policies
c) Unclear, I am not familiar with all the details
d) I am not aware of any specific policies

42. What would you do if you suspect that your computer or hospital device has been compromised (e.g., showing unusual behavior, acting slower)?
a) Report it to IT immediately
b) Try to fix it myself
c) Ignore it if I can still work
d) Reboot the device and continue working

43. Which of the following concerns do you feel are most significant for PET/CT systems? (Select all that apply)
a) Data privacy of patient scans
b) Vulnerabilities in equipment software
c) Unauthorized access to PET/CT machines
d) Use of unsecure devices (e.g., USBs)
e) Lack of cybersecurity policies
f) Other (Please specify)

44. Does your organization have cybersecurity protocols specific to medical devices like PET/CT systems?
a) Yes
b) No
c) Unsure/Don't know

45. Have you ever experienced a cybersecurity issue directly involving PET/CT equipment?
a) Yes
b) No
c) Unsure

SECTION 4: FEEDBACK AND ADDITIONAL COMMENTS

46. Which cybersecurity risks do you think are the most overlooked? (Select all that apply)
a) Phishing
b) Unauthorized device access
c) Unpatched vulnerabilities in medical devices
d) Poor password management
e) Insider threats
f) Lack of real time monitoring
g) Other (Please specify)

47. In your opinion, what improvements should be made to prevent phishing and other common cybersecurity threats? (Select all that apply)

a) More frequent training
b) Stricter password policies
c) Better access control for medical devices
d) Regular simulated phishing exercises
e) Enhanced incident reporting mechanisms
f) Other (Please specify)

48. What additional cybersecurity training or support would you find beneficial in your role?

a) More phishing detection training
b) Training on handling cybersecurity incidents
c) Hands on workshops for managing secure devices
d) General cybersecurity awareness
e) Other (Please specify)

49. How do you think cybersecurity risks in medical imaging could impact patient care and safety?

a) High impact on patient care and safety
b) Moderate impact on patient care
c) Low impact, but still a concern
d) No significant impact

50. What role should healthcare professionals play in improving cybersecurity within the hospital environment?

a) Actively participate in cybersecurity training
b) Report incidents and vulnerabilities
c) Collaborate with IT to ensure secure equipment usage
d) No specific role needed
e) Other (Please specify)