

**Horizon 2020 Marie Skłodowska-Curie**

**Research and Innovation Staff Exchange Evaluations (RISE)**



**A CybEr range tRaining platform for medicAl organisations and systems Security**

**D4.3: AERAS Cyber Range Tools – V2**

**Abstract**: This deliverable describes the final outcome of Task 4.1 and Task 4.2 and, updating deliverable 4.1 and describing in detail the cyber range infrastructure of AERAS.

|  |  |
| --- | --- |
| Contractual Date of Delivery | 15/06/2025 |
| Actual Date of Delivery | 15/06/2025 |
| Deliverable Security Class | Public |
| Editor | UMIL |
| Contributors | Theodoros Christophides, Kostas Iordanou, Ioannis Panagiotou (CUT)  Nastasia Michael, Panagiotis Archontidis (LIBRA)  Esftratios Syrmas, Ioanna Stamouli (UPAT)  Dimitrios Dounas, Nikolas Ioannou, Konstantinos Papadamou (TRID)  Fulvio Frati (UMIL) |
| Quality Assurance | Kostantinos Papadamou (TRID)  Pantelitsa Leonidou (CUT) |

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 |
| Trinomial Technologies LTD | TRID | Cyprus |
| Ethical AI Novelties | EAIN | Cyprus |
| Libra AI Technologies | LIBRA | Greece |

*Document Revisions & Quality Assurance*

**Internal Reviewers**

1. *Kostantinos Papadamou (TRID)*
2. *Pantelitsa Leonidou (CUT)*

**Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Overview** |
| 1.0 | 15/06/2025 | Editor | Version submitted |
| 0.7 | 01/06/2025 | Editor | Internal review |
| 0.5 | 15/05/2025 | Editor | Final Version of Deliverable |
| 0.3 | 15/04/2025 | Editor | Final version of Architecture |
| 0.2 | 15/03/2025 | Editor | Updated version with first draft of architecture |
| 0.1 | 15/01/2025 | Editor | First Draft of the table of contents |

*Executive Summary*

This deliverable describes the final AERAS Cyber Range and simulation tools, following the draft architecture depicted in D4.1. The deliverable give a throughout description of the final platform, along with the deep adaptations that has been needed to make the open source platform KYPO suitable for AERAS technical and training requirements. This deliverable has been written in strict correlation with WP5 team and in particular, it is connected with D5.3 describing the final deployment of the whole infrastructure in a real environment.

*Table of Contents*

Sommario

[1. Introduction 8](#_Toc199836894)

[1.1 Relations with other Deliverables 9](#_Toc199836895)

[2. The Implementation roadmap of AERAS platform 10](#_Toc199836896)

[2.1 Overview 10](#_Toc199836897)

[2.2 KYPO & KYPO LITE 12](#_Toc199836898)

[3. AERAS Cyber Range Core Engine (AERAS-CRCE) 16](#_Toc199836899)

[3.1 Cyber Range Objectives 16](#_Toc199836900)

[3.2 AERAS Cyber Range Platform: KYPO 17](#_Toc199836901)

[3.3 Training Execution 23](#_Toc199836902)

[4. Visualization Capabilities 28](#_Toc199836903)

[4.1 Feedback from the Practitioners 28](#_Toc199836904)

[4.2 Trainee and Trainer Interface 30](#_Toc199836905)

[5. Conclusions 34](#_Toc199836906)

[6. References 35](#_Toc199836907)

*List of Figures*

Figure 1: AERAS reference infrastructure. 9

Figure 2: AERAS actual architecture having KYPO at its core. 10

Figure 3: KYPO Cyber Range Platform Deployed Services 18

Figure 4. AERAS Platform User Groups/Roles View and Management 19

Figure 5. User Group/Role Management 19

Figure 6. AERAS Cyber Range Platform - Example list of Sandbox Definitions 20

Figure 7. AERAS Cyber Range Platform - Resource Pool Definition 21

Figure 8. AERAS Cyber Range Platform - Example list of defined Resource Pools 21

Figure 9. AERAS Cyber Range Platform - Example List of Training Definitions 22

Figure 10. AERAS Cyber Range Platform - User Authentication Screen 23

Figure 11. AERAS Cyber Range Platform - Main Screen of the Trainee/Simple User View 23

Figure 12: AERAS training exercise: Introduction page 24

Figure 13: AERAS training exercise: General description of the requested task 24

Figure 14: AERAS training exercise: starting of the training. 25

Figure 15: AERAS training exercise: VMs access interface. 26

Figure 16: AERAS training exercise: Hands-on exercise instructions 26

Figure 17: AERAS training exercise: access to VM. 27

Figure 18: Trainee view: user results with numerical scores. 31

Figure 19: Trainee view: user results with graphical trend. 31

Figure 20: Trainee view: user result with dotted view. 32

Figure 21: Trainer view: list of trainees' results. 33

Figure 22: Trainer view: results of awareness quiz. 34

*Table of Abbreviations*

|  |  |
| --- | --- |
| **AERAS-CRCE** | AERAS Cyber Range Core Engine |
| **WP** | Work Package |
| **CYRA** | Cyber Range Assurance Platform |
| **CRSA** | Cyber Range Security Assurance |
| **CRST** | Cyber Range Simulation and Training |
| **CSE** | Cyber System Emulator |
| **IDS** | Intrusion Detection Systems |
| **NCSC** | Czech National Cyber Security Center |
| **T&E** | Testing & Evaluation |
| **VM** | Virtual Machine |
|  |  |
|  |  |
|  |  |
|  |  |

# Introduction

The AERAS framework excels with its tools and procedures for continuous assessment of an organization's cybersecurity landscape and related risks. The project also enhances training effectiveness by adapting activities based on updated cybersecurity threats and trainee responses. AERAS adds value by evaluating training effectiveness through the organization's risk level before, during, and after the training. This correlation shows that as the organization’s cybersecurity improves, so does the effectiveness of the training.

**The primary** **role of this deliverable** is to update the content of D4.1 and describes the final outcomes of Task 4.1 and 4.2, depicting the final cyber range infrastructure used as AERAS training platform. This deliverable, starting form the high-level description given in the previous deliverable D4.1, go deep in analysing how KYPO has been adapted as included as official AERAS cyber range infrastructure, given its intrinsic ability to be adapted to different context and training topics.

The deliverable tackles the following AERAS objective, as stated in the project proposal.

|  |
| --- |
| ***“Objective 4:*** *Develop capabilities required for the delivery of effective cyber training, namely emulation, simulation, security assurance assessment, and visualisation capabilities.”*  This deliverable directly contributes to Objective 4 by detailing the development of the AERAS Cyber Range, which includes advanced emulation and simulation tools within the Cyber Range platform. These tools are designed to replicate cyber-system components and attack scenarios, providing a realistic training environment. Additionally, the deliverable outlines the creation of visualization components that offer real-time insights into cyber-system statuses and attacks. These capabilities are essential for effective cyber training, enabling trainees to engage in hands-on experiences and to assess security measures comprehensively. |

|  |
| --- |
| ***“Objective 5:*** *To integrate capabilities developed under Objectives 1-4 into a common platform that delivers realistic and highly adjustable cyber training, offering hands-on experience against cyber-attacks, and supporting decision making in employing different mixtures of security mechanisms to combat risks and to demonstrate and validate the use of the AERAS platform for realistic and highly adjustable cyber training in the critical healthcare sector using two separate pilots based on real systems at TRL 7.”*  The deliverable supports Objective 5 by laying the groundwork for integrating the developed emulation, simulation, and visualization capabilities into a cohesive training platform. This platform is designed to be highly adjustable and realistic, providing a comprehensive environment for cyber training. The detailed implementation of these tools ensures that the platform can simulate various cyber-attack scenarios and security mechanisms, thereby supporting decision-making processes. Furthermore, the deliverable sets the stage for the subsequent demonstration and validation of the AERAS platform in the healthcare sector, ensuring that it meets the requirements for realistic and effective cyber training at TRL 7, where the demo has been installed and validate within our two pilots. |

In the following sections, we describe as KYPO has been integrated and adapted in the AERAS infrastructure as depicted in the Figure 1 below (see the Cyber Range Core Engine and Visualisation component – enclosed in the red dashed line).

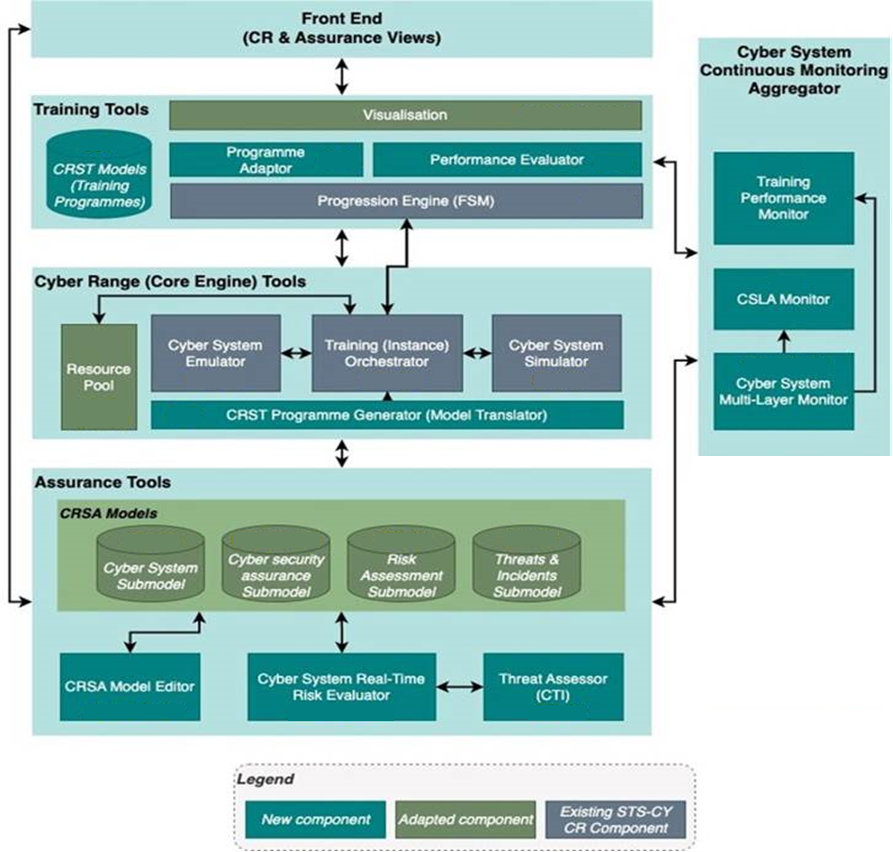


Figure 1: AERAS reference infrastructure.

## 1.1 Relations with other Deliverables

This deliverable is the updated and final version of D4.1 and will provide input to D4.4, which defines the application of the guidelines for training adaptation depicted in D4.2. Additionally, D4.3 significantly contributes to the final deliverables of WP5 by providing the foundational components and tools necessary for the infrastructure that will be subject to the experimentation. D5.3 has been coordinated with the finalization of D4.3, allowing a strict correlation within the secondments teams managing the development and the deployment of the infrastructure.

The rest of the deliverable is structured as follows: Section 2 presents a description of the actual implementation of the AERAS platform centered around the KYPO Cyber Range framework (KYPO), describing the process of selection of the reference architecture with respect to AERAS technical and training requirements.

Then, Section 3 presents the actual implementation, showing a selection of screenshots driving the readers into a real training exercise. Furthermore, Section 4 presents the visualization interfaces, both from the Trainee and the Trainer side, of the results of the training programme.

Finally, Section 5 draws our conclusions.

# 2. The Implementation roadmap of AERAS platform

## 2.1 Overview

Within WP4, the team has spent significant research effort for selecting, and developing, the best-fitting technologies that could be exploited to reach the ambitious goals of the AERAS framework. In particular, the **Cyber System Emulator** module is the core component that will drive the design of the other modules. The content of this section has not been updated from D4.1, since it gives a sound grounding on the discussion below about the integration of KYPO, justifying its selection.

An extensive analysis of the available cyber range frameworks identified the KYPO Cyber Range Platform [1,2] – recently released as open source – as the best candidate for inclusion. KYPO facilitates the creation of complex virtual cyber-systems and networks, with fully functional operating systems and network devices, while being fully model-based. This allows us to integrate the full range of its functionalities to our approach.

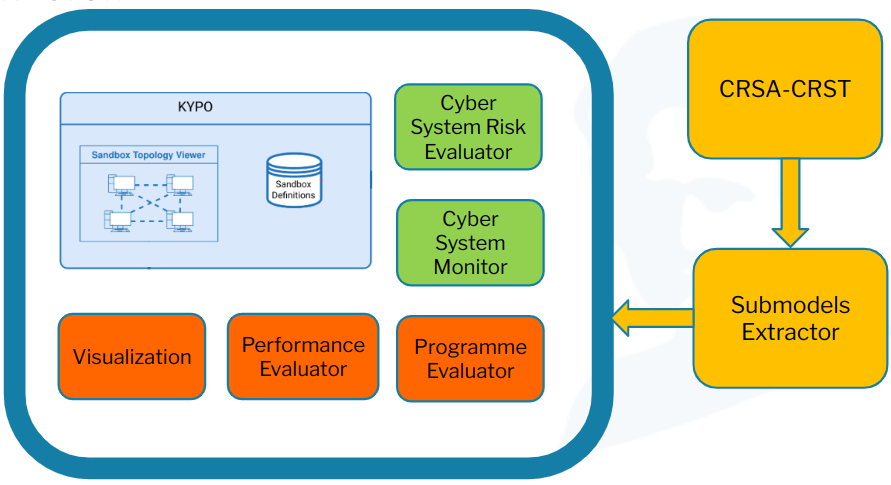


Figure 2: AERAS actual architecture having KYPO at its core.

In this context, the consortium is focused on designing the adaptation of KYPO models to the AERAS-specific CRSA and CRST models, defining techniques for the population of KYPO-specific instances with AERAS concept. Please see D3.3 for major details on this phase.

The AERAS cyber range platform (see Figure 2) will offer a comprehensive suite of modules an methodologies designed to enhance cybersecurity training and evaluation. First, we define the *CRSA-CRST models*, and we extract the relevant *Submodels.* Then, the *Cyber System Risk Evaluator* methodology enables a detailed assessment of potential risks within simulated environments, providing insights into vulnerabilities and threat impacts. The *Cyber System Monitor* offers real-time monitoring capabilities, allowing users to track network activities and detect anomalies as they occur. The *Visualization* module facilitates the exchange of information during training sections where trainees engage with it to deliver and respond to simulated cyber-attack scenarios. It enhances the user experience by presenting data through intuitive and interactive charts and graphs, making complex information more accessible. The *Performance Evaluator* methodology assesses the efficiency and effectiveness of cyber defenses and responses, ensuring that strategies are optimized for real-world scenarios. Finally, the *Programme Evaluator* methodology reviews and analyzes the overall training programs, providing feedback and metrics to ensure continuous improvement and alignment with cybersecurity best practices. Together, these modules create a robust and dynamic platform for cybersecurity professionals to hone their skills and improve their defensive strategies.

As we describe in the next paragraphs, a variety of different frameworks have been examined, but all lacked important properties, such as availability, community support, and documentation, which made them not fitting to be incorporated in the framework. Nevertheless, several high-level commercial and public cyber ranges are available on the market, each offering unique features and capabilities.

**Commercial Cyber Ranges**

*Cyberbit Cyber Range* [4] provides a training/simulation platform for the instantiation and management of hyper-realistic training centers. The *AIT Cyber Range* [5], offered by the Austrian Institute of Technology, provides a virtual environment for flexible simulation of critical IT systems. The *Virginia Cyber Range* [6] supplies a cloud-hosted virtual environment for training students in handling cybersecurity events. Similarly, the *Michigan Cyber Range* [7] focuses on strengthening the state's cyber defenses by providing one of the largest unclassified, network-accessible cybersecurity training platforms. The *National Cyber Range* (NCR) [6] enables realistic cybersecurity testing, evaluation (T&E), and training. In the private sector, the Italian Aerospace, Defence, and Security Company Leonardo offers a multipurpose operational environment that creates realistic operational training scenarios using best-of-breed technologies for Infrastructure-as-Code provisioning, cloud management, and software-defined networking [9].

**EU-Funded Cyber Ranges**

Many projects funded by the European Commission under the Horizon 2020 Framework Program have also produced high-quality cyber range platforms. *Cyber Range Assurance Platform* (CYRA) [3] trains trainees for known and new cyber-attacks by adapting to the evolving threat landscape and assessing if trainees transfer the acquired knowledge to their work environment. *THREAT-ARREST* [10] employs modern training methods, including emulation, simulation, serious gaming, and the fabrication of realistic synthetic data, to enhance the learning experience. The *SPIDER* cyber range [11] replicates a customized 5G network, enabling cyber-exercises that allow real-time hands-on interaction, information sharing between participants, and feedback gathering from network equipment, as well as the development and adaptation of advanced operational procedures.

The *CYBERWISER* cyber range platform [12] offers a multipurpose virtual environment where organizations can test critical capabilities and evaluate how effectively they integrate people, processes, and technology to protect strategic information, services, and assets. Ukwand et al. [13] documented cyber range and test-bed platforms, characterizing them by type, technology, threat scenarios, applications, and the scope of attainable training. This analysis is enriched by a taxonomy developed to provide a broader understanding of future environments. Somarakis et al. [14] describe the link between Cyber Range training and Assurance, introducing a model-driven approach that facilitates the generation of ad-hoc training scenarios based on a comprehensive model-based description of the organization and its security posture. Additionally, Cybersecurity training through Cyber Range has been exploited for critical environments. For example, the *Cyber Arena* environment [15] integrates ICT architectures of multiple organizations, modelling enterprise interdependencies of ICT architecture and business, as well as internet and cloud architectures at different tier levels, to create a complex training environment in the cybersecurity domain.

In the following sections, we provide the implementation roadmap for the emulation, simulation, and visualization components of AERAS. This detailed plan will highlight how the AERAS platform, centered around KYPO, ensures comprehensive cybersecurity training and risk assessment.

## 2.2 KYPO & KYPO LITE

The **KYPO Cyber Range Platform (KYPO)** is a comprehensive and advanced tool designed for cybersecurity training, research, and testing. Developed by the Czech National Cyber Security Center (NCSC). It provides a simulated environment where users can practice defending against cyber threats in a realistic and controlled setting. The platform is used by a variety of stakeholders, including government agencies, academic institutions, and private companies.

In this section, we present the key features and properties that rendered KYPO as the best fitting core technology for the AERAS cyber range tools.

Key features of the KYPO include:

1. **Realistic Simulations**: KYPO offers realistic cyber-attack scenarios, allowing participants to experience and respond to genuine cyber threats. This helps in enhancing the skills and readiness of cybersecurity professionals.
2. **Customizable Environments**: Users can create and customize their own network environments and scenarios to match specific training needs or research objectives. This flexibility makes it suitable for a wide range of applications.
3. **Shared Training Scenarios:** Multiple trainees could run through the same scenario independently and then compare their results or discuss their thought processes after the fact.
   1. **Independent Runs:** KYPO allows the creation of repeatable training scenarios. This means multiple trainees can independently run through the same simulated environment and encounter the same challenges.
   2. **Post-Training Collaboration:** While the platform itself might not facilitate live collaboration during the scenario, trainees can still compare their results and discuss their thought processes after completing the exercise. This allows them to learn from each other's approaches and identify areas for improvement.
4. **Educational Integration**: KYPO is designed to support educational institutions by providing tools and resources for cybersecurity education. It integrates with various teaching methods and curricula, helping to prepare students for careers in cybersecurity.
5. **Research and Development**: Researchers can use KYPO to test new cybersecurity tools, techniques, and strategies in a safe environment. This capability supports innovation and the development of cutting-edge cybersecurity solutions.
6. **Scalability**: The platform is scalable, accommodating a range of users from small teams to large organizations. This ensures that it can grow with the needs of its users.
7. **User-friendly Interface**: KYPO features an intuitive interface that makes it accessible to users with varying levels of technical expertise. This ease of use encourages broader participation and more effective training.

|  |
| --- |
| **In summary**, the KYPO Cyber Range Platform is a powerful resource for enhancing cybersecurity skills, fostering collaboration and innovation, and supporting research and education in the field of cybersecurity. |

**KYPO Lite** is a streamlined version of KYPO designed to offer essential cybersecurity training and simulation capabilities in a more accessible and user-friendly package. It is aimed at smaller organizations, educational institutions, and individuals who need robust cybersecurity training tools without the complexity and resource requirements of the full KYPO platform.

Key features of KYPO Lite include:

1. **Simplified Setup**: KYPO Lite is designed for quick and easy deployment, making it accessible for users with limited technical resources or expertise. This allows for immediate use in various environments.
2. **Core Training Scenarios**: The platform includes a selection of core cybersecurity scenarios that cover fundamental attack and defense techniques. These scenarios provide practical, hands-on experience in dealing with common cyber threats.
3. **User-Friendly Interface**: With an intuitive and straightforward interface, KYPO Lite is designed to be easy to navigate, ensuring that users can focus on training rather than managing complex systems.
4. **Educational Focus**: KYPO Lite is particularly suited for educational purposes, providing students and instructors with a valuable tool for learning and teaching cybersecurity principles. It supports classroom integration and can be used to complement theoretical learning with practical exercises.
5. **Cost-Effective**: As a lighter version of the full platform, KYPO Lite is more cost-effective, making advanced cybersecurity training accessible to a broader audience, including smaller organizations and educational institutions with limited budgets.
6. **Scalability and Flexibility**: Although designed as a lighter version, KYPO Lite retains the flexibility to scale up in complexity and size as needed, ensuring it can adapt to growing training requirements.

|  |
| --- |
| **In summary,** KYPO Lite offers a practical and accessible solution for cybersecurity training, focusing on essential features and ease of use. It serves as an excellent tool for smaller organizations and educational institutions looking to enhance their cybersecurity capabilities without the need for extensive resources. |

The key differences between KYPO and KYPO Lite are discussed in the following Table 1:

|  |  |
| --- | --- |
| **Table 1: KYPO versus KYPO Lite** | |
| **1. Complexity and Features:** | |
| **KYPO:** Offers a comprehensive set of features and tools for advanced cybersecurity training, research, and testing. It includes a wide range of customizable scenarios, realistic simulations, and extensive collaboration and competition options. | **KYPO Lite:** Focuses on providing essential cybersecurity training tools with a simplified setup and user-friendly interface. It includes core training scenarios but lacks some of the advanced customization and extensive feature sets of the full KYPO platform. |
| **2. Target Audience** | |
| **KYPO:** Aimed at a broad range of users, including government agencies, large organizations, academic institutions, and cybersecurity professionals who require advanced capabilities for training, research, and development. | **KYPO Lite:** Designed for smaller organizations, educational institutions, and individuals. It is ideal for those needing a cost-effective, easy-to-deploy solution for fundamental cybersecurity training. |
| **3. Deployment and Setup** | |
| **KYPO:** Requires more extensive technical resources and expertise for deployment and management. It is designed for use in larger, more complex environments. | **KYPO Lite:** Features a simplified and quick deployment process, making it accessible for users with limited technical resources or expertise. |
| **4. Potential costs related to infrastructure, technical expertise, customization, and support** | |
| **KYPO:** Generally higher in cost due to its advanced features and extensive capabilities, suitable for users with larger budgets and more comprehensive training needs. | **KYPO Lite:** More cost-effective, making it accessible to smaller organizations and educational institutions with limited budgets. |
| **5. Customization and Scalability** | |
| **KYPO:** Highly customizable with the ability to create tailored scenarios and environments. It is scalable to accommodate large numbers of users and complex setups. | **KYPO Lite:** Offers essential customization options but is more limited compared to the full KYPO platform. It is scalable to some extent but designed primarily for smaller-scale use. |
| **6. Educational Integration** | |
| **KYPO:** Supports a wide range of educational and training methods, including integration with advanced curricula and research projects. | **KYPO Lite:** Specifically tailored for educational purposes with straightforward integration into classroom settings, focusing on fundamental cybersecurity principles. |
| **7. Research and Development** | |
| **KYPO:** Provides robust tools for cybersecurity research and development, allowing users to test new tools, techniques, and strategies in a secure environment. | **KYPO Lite:** Primarily focused on training rather than advanced research, offering essential tools and scenarios for practical learning experiences. |

In summary, KYPO is a full-featured, advanced platform designed for comprehensive cybersecurity training and research, suitable for larger organizations and professional use. KYPO Lite, on the other hand, provides a simplified, cost-effective solution focusing on essential training needs, ideal for smaller organizations and educational institutions.

**Advantages**

We have selected KYPO as the core technology for the AERAS cyber range tools due to its modularity, adaptability, and open-source nature. These features make KYPO highly customizable and easy to integrate with AERAS specific training requirements.

Additionally, its proven effectiveness in supporting diverse cybersecurity scenarios ensures that it meets our comprehensive training needs. The detailed explanation of these advantages will be provided in the following Section 3.

Finally, among several commercial solutions, KYPO stands up as a concrete open-source solution ready to be integrated and included in research projects like AERAS.

**Implementation Roadmap**

In the first implementation phase, the AERAS team has evaluated the KYPO LITE capabilities for integrating the AERAS modules. This initial evaluation has focused on ensuring compatibility and identifying any potential challenges in the integration process. The second step involved incorporating the full KYPO framework, which will provide enhanced features and greater flexibility for creating complex virtual networks with fully functional operating systems and network devices.

With this plan in mind, the AERAS cyber range platform has been adapted taking KYPO at its core. By starting with KYPO LITE, the team can gradually build up to the full capabilities of the KYPO framework, ensuring a smooth and effective implementation process. This approach will allow the AERAS platform to leverage the strengths of KYPO, resulting in a robust and versatile cyber range environment that meets the specific needs of the project.

**Challenges in KYPO installation**

On the other side, KYPO, being an open-source platform, offered insights into its workings and capabilities through installation. However, deploying and configuring KYPO has presented significant challenges for the developing and the deployment teams, particularly in meeting DevOps-level requirements such as OpenStack integration.

Following KYPO's documentation step by step revealed compatibility issues between older and newer versions, prompting attempts to adapt configurations without pinpointing the core issue. While KYPO support provided valuable guidance, navigating through unclear sections of the documentation necessitated consulting additional resources like OpenStack documentation.

As described in D5.3, the team needed to undergo several development cycles to adapt KYPO drivers and modules to the latest OpenStack infrastructure version, sorting out several installation and integration issues. This work has been considered a strong effort and outcomes of the AERAS project, proving to the community the adapted modules for further installation of the full KYPO infrastructure.

# 3. AERAS Cyber Range Core Engine (AERAS-CRCE)

In this section we provide the description of the adaptation of the KYPO platform to the AERAS technical and training requirements.

**Emulation** and **simulation** are two crucial components of the AERAS Cyber Range Core Engine (see Figure 1) and serve different purposes. However, both are integral to creating effective cybersecurity training environments.

**Emulation** involves creating an environment that behaves like a real-world system. This includes full-fledged operating systems, network devices, and applications, all running on virtual machines within isolated sandboxes. These emulated environments allow users to interact with systems as they would in a real-world scenario, providing a high degree of realism for hands-on cybersecurity training and exercises. This approach ensures that the training is as close to actual operational conditions as possible, making it highly effective for teaching practical skills and conducting realistic cybersecurity exercises​.

**Simulation**, on the other hand, generally involves creating a model of a system that can mimic its behaviour under certain conditions but does not necessarily replicate the full functionality of real systems. In the context of KYPO, simulations might be used to create specific scenarios or to model the effects of cyber-attacks on a network without the need for a full-scale emulation of every component. This can be useful for understanding the impacts of certain actions or for running large-scale exercises where full emulation would be too resource-intensive​​.

## 3.1 Cyber Range Objectives

In this section, we provide a detailed overview of the emulation objectives of the AERAS Cyber Range Core Engine (AERAS-CRCE) should provide and are implemented by the KYPO installation. The objectives were identified and described in D4.1, and drove the selection of KYPO as AERAS cyber range solution.

The objective were organized in two categories: *Emulation* and *Simulation* capabilities.

Among the Emulation capabilities we could find the following:

**1. Provide a realistic Network Environments:** emulation of complex network environments that closely resemble real-world IT infrastructures, including servers, workstations, routers, and other network devices. This allows users to interact with systems and networks as they would in actual operational environments.

**2. Operating Systems and Applications:** emulation of various operating systems (e.g., Windows, Linux) and applications, enabling users to simulate diverse environments and scenarios. This is crucial for practicing responses to threats across different platforms and software.

**3. Virtual Machines:** usage of different virtual machines (VMs) to emulate different endpoints and network components.

**4. Network Traffic and Protocols:** emulation of network traffic and protocols, allowing users to observe and analyze typical and atypical network behaviors. This includes the ability to inject malicious traffic to study how attacks propagate and impact the network.

Emulation objectives include the possibility to replicate various cyber-attack scenarios, the deployment and testing of defensive measures, the execution of incident response processes, and the creation of training and assessment exercises, tailored for the project pilots.

The Simulation capabilities included the following:

**1. Cyber Attack Scenarios:** simulation of real cyber-attack scenarios, including malware infections, denial-of-service attacks, phishing campaigns, and more, to allow trainees to how to tackle them.

**2. Defensive Measures:** simulation of the deployment and effectiveness of various defensive measures such as firewalls, Intrusion Detection Systems (IDS), and antivirus software, to train on the evaluation of different defensive strategies and configurations.

**3. Incident Response:** simulation of incident response processes, allowing teams to practice identifying, containing, and mitigating security incidents.

**4. Training and Assessment:** creation of training exercises and assessments. Participants can be evaluated on their ability to detect, respond to, and recover from simulated cyber incidents. This is valuable for both individual skill development and team-based exercises.

**6. Scenario Customization:** matching of pilot training requirement and AERAS training proposals.

## 3.2 AERAS Cyber Range Platform: KYPO

As described in the previous sections, As part of the AERAS platform architecture, the KYPO[[1]](#footnote-2) Cyber Range Platform has been selected and deployed as the foundational cyber range environment to support simulation-based cybersecurity training and experimentation. KYPO, originally developed by Masaryk University and released as an open-source project, is a modern, container-based cyber range management system designed to orchestrate and manage complex cybersecurity training scenarios in a scalable, modular, and reproducible fashion.

KYPO provides a robust, extensible framework for defining, deploying, and managing cyber exercises, offering instructors and platform administrators the ability to tailor networked environments that emulate realistic ICT infrastructures and adversarial scenarios. Its containerized backend architecture and reliance on infrastructure-as-code principles make it particularly well-suited for integration into heterogeneous environments such as AERAS, which emphasizes modular security assurance tooling, federated data flows, and dynamic training feedback loops.

In the context of AERAS, KYPO has been deployed not simply as a standalone cyber range, but as a core component of the Training Tools Layer within the broader multi-layered AERAS architecture. Its role is to serve as a programmable environment for delivering customized cyber resilience scenarios tailored to the evolving needs of the healthcare and other critical sectors. More specifically, KYPO supports the dynamic provisioning of training programs aligned with the CRSA and CRST models employed by AERAS, enabling evidence-based evaluation of both technical and human factors in organizational cybersecurity posture.

Being an open source framework, the adaptation of KYPO to the AERAS technical requirements requires an extensive work in terms of redefinition of models and modules, as well as the implementation and integration of new software. In the following, we will provide a detailed description of the results of the work the development team within WP4.

Figure 3 below initially depicts the list of services which have been deployed and together form the AERAS Cyber Range Platform, where the sandboxes manages the actual separated environments that runs the training exercises.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : KYPO Cyber Range Platform Deployed Services

The figures below illustrate the administrative interface of the AERAS Cyber Range Platform.

This interface enables platform administrators to configure and manage core components essential for the execution of training programs. Initially, administrators can create and manage user accounts and organize users into groups as shown in Figure 4 and Figure 5.

A screenshot of a group overview

AI-generated content may be incorrect.

Figure 4. AERAS Platform User Groups/Roles View and Management

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5. User Group/Role Management

Furthermore, the AERAS Cyber Range Platform incorporates a comprehensive suite of functionalities that empower administrators to define and manage key training infrastructure components, including sandboxes, resource pools, and training scenarios. These elements constitute the foundational framework required to design, orchestrate, and deploy advanced CRST programs. Their configuration and interplay ensure that training activities are not only operationally coherent but also strategically aligned with the broader AERAS methodology for cyber risk assessment and organizational resilience enhancement.

At its core, a sandbox—also referred to as the Cyber System Emulator (CSE) within the AERAS Platform architecture—serves as a formal definition and virtual replication of an organization’s cyber infrastructure, or a selected segment thereof, used within the scope of a training program.

Functionally, the sandbox encapsulates the network topology of the target environment, detailing all constituent elements such as servers, client machines, routers, switches, and other network devices, along with their interconnections and configurations. These sandbox definitions are integral to AERAS training programs, as they provide the virtualized environment in which cyber resilience scenarios are executed. They allow for realistic emulation of operational networks, enabling trainees to engage in hands-on exercises that accurately reflect the complexity and heterogeneity of real-world infrastructures. Figure 6 depicts an example of some of the sandbox definitions in AERAS.

A screenshot of a computer

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - Example list of Sandbox Definitions

In addition, the AERAS platform provides robust capabilities for creating and managing resource pools through the Training Instance Orchestrator component. A resource pool, also referred to as a sandbox pool, represents a live, instantiated version of a predefined sandbox. It includes all associated virtual machines, networked components, and computing resources defined in the corresponding sandbox topology, provisioned and allocated for active use in training scenarios.

These resource pools are essential for the operationalization of training programs, as they provide isolated, fully functional environments in which trainees can interact with realistic infrastructure replicas under controlled conditions. The dynamic provisioning and lifecycle management of these pools ensure scalability, repeatability, and consistency across different training sessions and organizational contexts. Figure 7 presents the interface for defining a new resource pool, while Figure 8 provides an overview of existing resource pools managed within the AERAS Cyber Range platform.

A screenshot of a computer

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - Resource Pool Definition

A screenshot of a computer

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - Example list of defined Resource Pools

Moreover, the AERAS platform provides administrator users and designated training instructors with the ability to create, view, and manage CRST models and corresponding training program definitions. A training definition encapsulates the structure and content of a complete training program, including the instructional description presented to trainees, the sequential flow of training steps, and the configuration of interactive exercises and assessment components.

Each training definition is designed to guide the trainee through a series of learning stages—comprising practical tasks, decision-making scenarios, and knowledge-based questions—which collectively contribute to the final performance evaluation. The system allows for granular customization of these elements to align with organizational learning objectives and CRSA-aligned training goals.

Figure 9 illustrates the training definitions management interface within the AERAS platform, showcasing a sample list of defined programs along with the available options for editing, deploying, or archiving each training definition.

A screenshot of a computer

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - Example List of Training Definitions

Furthermore, the AERAS platform is also accessible by simple users (or trainees) who access the platform to perform a training given the necessary credentials and training program access tokens provided by an instructor or an administrator. Trainee accounts can only be created by administrators and/or instructors.

Figure 10 shows the authentication screen that the user sees when trying to access the platform, while Figure 11 shows what a trainee sees after logging in to the AERAS platform to perform a training program.

A screenshot of a login screen

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - User Authentication Screen

A screenshot of a computer

AI-generated content may be incorrect.

Figure . AERAS Cyber Range Platform - Main Screen of the Trainee/Simple User View

## 3.3 Training Execution

In the following sections we provide the readers with an examples of training implemented within the AERAS platform. The training has been configured by populating the KYPO models taking into account CRSA and CRST developed in WP3, and derived from the training requirements analysis. All the exercise is created using the platform interface for the creation of a training sandbox, a separated and isolated space that will contain all the exercise artifacts (VMs, quizzes, questionnaires, …). Furthermore, the sandbox execution represents an implementation of the phase 3 and 4 of the checklist described in D4.2 and D4.4.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12: AERAS training exercise: Introduction page

First, the trainee lands in a welcome page where the context of the exercise is introduced (see Figure 12). An initial high level description is given, trying to introduce the trainee in the context of the provided exercise. In this case, we describe what is intended as “Phishing Attack” and we list the expected objectives of the training.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : AERAS training exercise: General description of the requested task

Then, the next page shown in Figure 13 and Figure 14 introduce more deeply the trainee into the exercise describing the step of the investigation that will constitute the exercise itself.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : AERAS training exercise: starting of the training.

To finally execute the exercise, the trainee will be able to enter the specific VM created for this exercise. The interface in Figure 15 describes the underlying virtual network, created by the trainers in order to make the exercise more realistic. In fact, the KYPO sandboxes could theoretically replicate complex real-world network infrastructure, allowing the trainees to operate like they were at their real workstation.

It is important to note that the virtual network is based on the information that have been included and collected during the CRSA population phase of the AERAS checklist (see D4.2). In fact, the AERAS approach can drive the trainers in the analysis of the whole working environment, identification of the major training requirements via the RiskFactor analysis (see D4.2 and D4.4), and deploy the most suitable training experience with tailored and realistic virtual environments.

Then, Figure 16 goes deeply in the description of the required exercise steps, as expected by the trainers.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : AERAS training exercise: VMs access interface.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : AERAS training exercise: Hands-on exercise instructions

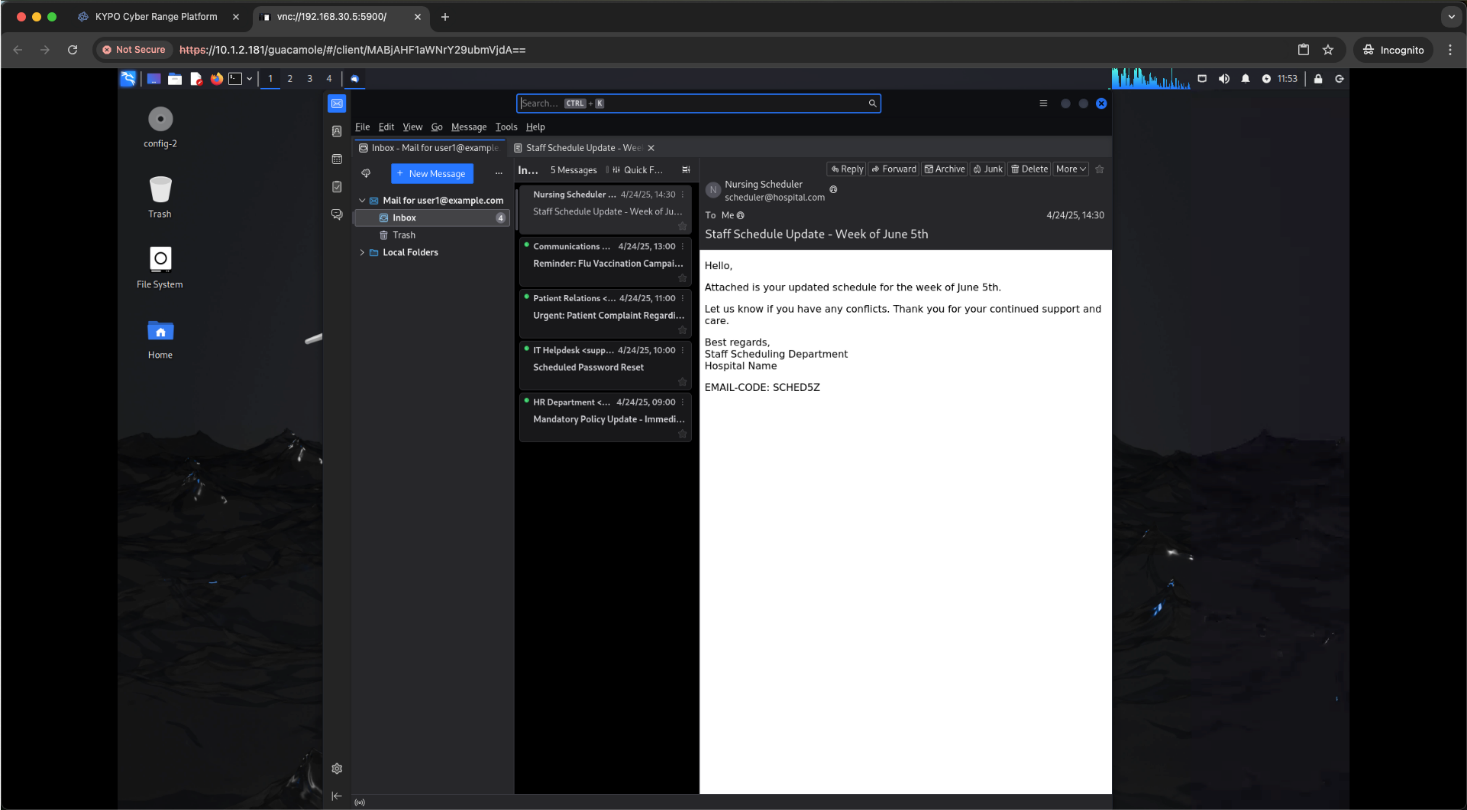


Figure : AERAS training exercise: access to VM.

Finally, Figure 17 show the actual access interface to the VM associated to the training program. In this exercise, trainee will be faced with examples of phishing emails inside a real mail client program, like he was in the real working environment.

The trainee should use the knowledge he acquired during the training or during her/his working experience, and point out the legitimate and the fraudulent emails.

# 4. Visualization Capabilities

In D4.1, in collaboration with WP2 team, we take over focus groups and analysis with pilots in order to find out specific technical requirements for the platform. In this context, we listed a subset of them that were mainly focused on the visualization capabilities the platform should be equipped with. To ground the discussion regarding the actual trainee and administration interface, we keep the section and update it with the actual interfaces showing the status of the training from both the trainer and the trainee sides.

In particular, the AERAS platform incorporates advanced visualization capabilities designed to enhance user experience through clear, intuitive, and interactive representations of network environments, attack scenarios, and security operations. These visualizations play a crucial role in facilitating the understanding of complex cybersecurity concepts and in enhancing training effectiveness. The analysis process has been composed of interviews with professionals inside the pilots, discussion in focus groups, and analysis of the findings.

## 4.1 Feedback from the Practitioners

To define the functionalities of the AERAS cyber range platform, the WP2-4 team conducted a focus group on September 19th, 2023. The session engaged four practitioners and experts, primarily security professionals with expertise in the medical domain. The agenda included an introduction to the AERAS Platform, brainstorming sessions, initial mock-ups, user story discussions, and the collection of socio-demographic information. This collaborative effort aimed to gather insights and define essential features that will shape the development of the AERAS cyber range platform to meet the specific needs and challenges identified by our expert panel.

The four interviewees come from diverse backgrounds and expertise. The first interviewee is a 42-year-old Greek male based in Cyprus, working as a Security Expert in a company with 17 years of experience, contributing to user stories 1.1 to 1.5. The second interviewee is a 26-year-old Cypriot female residing in Cyprus, employed as a Special Scientist Researcher in Computer Engineering and Informatics at a university, with 3.5 years of experience, contributing to user stories 2.1 to 2.5. The third interviewee is an Italian male from Italy, affiliated with a university, contributing to user stories 3.1 to 3.3. Lastly, the fourth interviewee is a 35-year-old Greek male from Greece, working as a Medical Physics Researcher at a university with 5 years of experience, contributing to user stories 4.1 to 4.5.

In the following, we provide the key findings we were able to distil from the focus groups and discussions, categorizing them from the point of view of Trainees and Trainers.

|  |
| --- |
| **Key Findings** |
| **Trainee**  1.1 Training Program Selection:   * View all available training programs with details such as previous training history, scores, and deadlines. * Ability to select the desired training program for the current session.   1.2 Training Performance Tracking:   * Access key performance metrics for training sessions, including average completion rates, total training taken, hours spent training, and performance progression over time. * Compare personal performance metrics with peers.   2.3 Trainee Feedback:   * Receive detailed feedback on mistakes made during training scenarios or tests, including explanations of correct responses.   2.4 Training Overview:   * View comprehensive information about upcoming training modules, including titles, descriptions, levels, covered vulnerabilities, estimated completion times, evaluation types, and prerequisite orders.   2.5 Trainee Notifications:   * Receive notifications regarding training progress, scores, completed modules, ongoing modules, and reminders for deadlines. |
| **Trainer**  1.3 Training Program Management:   * View, edit, create, and assign training programs. * Access individual statistics for each program, including number of completions, average trainee performance, and average completion times.   1.4 Training Program Monitoring:   * Monitor progress of ongoing training programs, including trainee participation and progress. * Intervene in training programs by injecting events if necessary.   1.5 Training Program Evaluation:   * Assess overall trainee performance and training program effectiveness through detailed statistics. * Evaluate performance trends across different employee types or departments.   2.1 Overall and Individual Training Progress:   * Monitor ongoing training progress at an organizational level. * View average statistics and detailed metrics for individual trainees.   2.2 Assignment of Training:   * Access lists of trainees categorized by role or department. * Assign training courses/modules based on roles efficiently.   3.1 User-Friendliness:   * Ensure easy navigation to training information and scenarios for both trainers and trainees. * Provide clear overviews of training activities with minimal clicks.   3.2 Back Office Training:   * Develop training activities tailored to specific back-office tasks, such as handling phishing attacks.   3.3 Trainee Interface:   * Track trainee progress comprehensively, including course completion attempts, time spent, and detailed interaction metrics.   4.1 Threat Awareness Dashboard:   * Implement a strict patch management process to maintain system and software security.   4.2 Interactive Training Modules:   * Regular testing of disaster recovery and backup systems is conducted to ensure data integrity.   4.3 Incident Response Simulation:   * Develop interactive training modules with multimedia elements and real-life scenarios to engage learners effectively.   4.4 Vulnerability Assessment Tool:   * Implement a robust tracking system to monitor employee progress and performance metrics.   4.5 Reporting and Analytics:   * Collect feedback from trainees via surveys to continuously enhance training modules and programs. |

In summary, based on the feedback from the interviewees, the key points can be summarized in the following objectives that the AERAS visualization should achieve.

**Interface Expectations**

* User-friendly and simple interface that highlights the list of exercises.
* Real work environment interfaces are similar to tools typically used by trainees.
* Specific pages are dedicated to each exercise.
* Progress bar to track course completion.
* Quick interface to view assigned training without a specific order.
* Separate pages for detailed descriptions and instructions of training.

**General Requirements**

* Different user levels (novice to expert) with exercises tailored based on acquired skills.
* Exercises are categorized by specialty, department, and role.
* Methodology to weight results based on scenario difficulty and role.
* Use of icons instead of text for training exercises.
* Capability to communicate with admins during training.
* Reward system with badges for high-performing trainees.
* Option to add certificates for completed training, with sharing/download features.

**Course Overview**

* A clear view of exercises to be completed.
* Detailed exercise descriptions, including keywords, evaluation types, outcomes, and required skills.
* Assurance level indicators (e.g., red-green lights) for overall company assurance.
* Hints button is available for each training exercise.
* Security controls covered by each training clearly indicated.

**Trainer Overview**

* Access to statistics on topics and training covered by employees.
* Monitor exercise advancements and completion times.
* Overall grades and scores for exercises are visible.
* Capability to assign exercises and manage training programs effectively.

**Trainee Overview**

* Access to personal performance statistics such as completion rates, hours spent training, and score progression.
* Ability to track completed exercises and review feedback on mistakes.
* View of upcoming trainings and deadlines.

## 4.2 Trainee and Trainer Interface

In the following we presents the main trainee and trainer interface that show the progress of the training programme. The screenshots have been taken after several rounds of trainings by the employees involved in pilots’ evaluation.

*~~Immagine che contiene testo, schermata, numero, software

Il contenuto generato dall'IA potrebbe non essere corretto.~~*

Figure : Trainee view: user results with numerical scores.

Figure 18, Figure 19, and Figure 21 show the actual results achieved by “UPAT USER18” (all pilots’ tests have been executed with full anonymity to avoid any privacy concern). In particular, Figure 18 shows the composition of the trainee’s score for each exercise she/he has execute.

*~~Immagine che contiene testo, schermata, diagramma, schermo

Il contenuto generato dall'IA potrebbe non essere corretto.~~*

Figure : Trainee view: user results with graphical trend.

Then, Figure 19 shows the progress of trainee’s execution of the exercise and how this has evolved in time. This could suggests how much time the trainee has dedicated to a specific part and in which she/he found more problems and obstacles.

Finally, Figure 20 uses a dotted view to compare the results with average time and other players time, that will be populated after several future rounds of the training.

*~~Immagine che contiene testo, schermata, design

Il contenuto generato dall'IA potrebbe non essere corretto.~~*

Figure : Trainee view: user result with dotted view.

The Trainer’s interface aims at giving an holistic and complete view on the progress of the training, taking into account all the trainees that are participating. This to allow to trainers to monitor the advancement of the single trainee and the progress of the training programme as a whole.

Figure 21 gives the full status of trainees progress, with reference to a specific exercise. Each trainee is referred with a specific icon and the interface, among several information, specify the time needed to each trainee to complete the exercise and the grade he took.

Finally, Figure 22 shows the final results of the awareness quiz that was related to the Phishing attack exercise. Each dot identify the correct answer by a single trainee, giving a complete glimpse on the level of each student and of the class as a whole.

*~~Immagine che contiene testo, schermata, software, Icona del computer

Il contenuto generato dall'IA potrebbe non essere corretto.~~*

(a)

Immagine che contiene schermata, testo

Il contenuto generato dall'IA potrebbe non essere corretto.

(b)

Figure : Trainer view: list of trainees' results.

*~~Immagine che contiene testo, schermata, software, Icona del computer

Il contenuto generato dall'IA potrebbe non essere corretto.~~*

Figure : Trainer view: results of awareness quiz.

The selection of KYPO as reference architectures has taken into account also the availability of trainers’ and trainees’ visualization that can cover almost all the requirements specified in Section 3.1. Future development in the AERAS platform could involve major specific and more detailed results views, taking into account also the role of the trainees within the healthcare organization they belong to.

# 5. Conclusions

In conclusion, the deliverable successfully presented the final development of the AERAS Cyber Range, simulation tools, and visualization components. The work has been carried out with success by the WP4 deeply modifying and deploying the KYPO open source framework, taking into consideration AERAS project objectives.

In particular, Task 4.1 laid the groundwork for emulating and simulating various cyber-system components and attack scenarios, creating a robust training environment. Concurrently, Task 4.2 has focused on crafting an intuitive and customizable visualization environment, enhancing trainees' ability to monitor and interpret cyber-system statuses and attack vectors in real time.

The implementation marks significant progress towards a common and fully reusable cyber range for the healthcare sector, along with the full AERAS methodology described in D4.2 and implemented in WP4 and WP5, exploiting the models defined and populated in WP3.

# 6. References

1. CELEDA, P., CEGAN, J., VYKOPAL, J., TOVARNÁK, D.: Kypo- a platform for cyber defence exercises. In: STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming,Logistics, Cyber Defence. Munich (Germany): NATO Science and Technology Organization, pp. 1–12. NATO (2015)
2. https://crp.kypo.muni.cz/
3. Smyrlis, M., Somarakis, I., Spanoudakis, G., Hatzivasilis, G., Ioannidis, S.: CYRA: A model-driven cyber range assurance platform. Applied Sciences 11(11) (2021). DOI 10.3390/app11115165. URL https://www.mdpi.com/2076-3417/11/11/5165
4. https://www.cyberbit.com/
5. https://cyberrange.at/
6. https://virginiacyberrange.org/
7. https://www.merit.edu/cyberrange
8. https://www.peostri.army.mil/national-cyber-range-ncr
9. <https://shorturl.at/hvzAY>
10. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T., Goeke, L., Pape, S., Blinder, O., Vinov, M., Leftheriotis, G., Kunc, M., Oikonomou, F., Maglio, G., Petrarolo, V., Chieti, A., Bordianu, R.: The THREAT-ARREST cyber range platform. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp.422–427 (2021). DOI 10.1109/CSR51186.2021.9527963
11. Rebecchi, F., Pastor, A., Mozo, A., Lombardo, C., Bruschi, R., Aliferis, I., Doriguzzi-Corin, R., Gouvas, P., Alvarez Romero, A., Angelogianni, A., Politis, I., Xenakis, C.: A digital twin for the 5g era: the spider cyber range. In: 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 567–572 (2022). DOI 10.1109/WoWMoM54355.2022.00088
12. Basile, M., Dini, G., Varano, D.: CYBERWISER.eu: Innovativecyber range platform for cybersecurity training in industrial systems. Electronic Communications of the EASST79, 1–12 (2020).https://doi.org/10.14279/tuj.eceasst.79.1114.1065
13. Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kaval-lieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I.,Bellekens, X.: A review of cyber-ranges and test-beds: Currentand future trends. Sensors20(24) (2020).https://doi.org/10.3390/s20247148
14. Somarakis, I., Smyrlis, M., Fysarakis, K., Spanoudakis, G.: Model-driven cyber range training: A cyber security assurance perspective.In: Computer Security, pp. 172–184. Springer International Publishing (2020)
15. Karjalainen, M., Kokkonen, T.: Comprehensive cyber arena; thenext generation cyber range. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 11–16(2020).<https://doi.org/10.1109/EuroSPW51379.2020.00011>

1. https://crp.kypo.muni.cz/ [↑](#footnote-ref-2)