February 2025

AERAS

NewsLetter #4

AERAS

A CybEr range tRaining platform for medicAl organisations and systems Security

AERAS Concept & Approach

AERAS aims to develop a realistic and rapidly adjustable cyber range platform for systems and organizations in the critical healthcare sector, to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical cyber-systems and organizations against advanced, known, and new cyberattacks, and reduce their security risks. The platform will be a virtual cyberwarfare solution enabling the simulation of the operation and effects of security controls and offering hands-on training on their development, assessment, use, and management.

PROJECT OBJECTIVES

Develop and deliver a highly adaptive and person-centric service to support older adults in work life by creating a positive work environment for employee wellbeing.

Develop smart environment technologies to improve occupational safety and health.

Enhance the perception and cognition of smart devices towards human-centered and intuitive human-computer interaction.

Develop and validate a solution in real-world environments, capitalizing on ICT innovations that will increase the competitiveness of EU industry by accommodating the ageing workforce.

Guarantee cost-effectiveness and create socio-economic benefits.

AERAS has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 872735.

AERAS

Consortium

The consortium consists of 9 partners from Academia and Industry from 4 EU countries (Italy, Greece, Cyprus, Germany):

UNIVERSITÀ DEGLI STUDI DI MILANO

Universita Degli Studi Di Milano (UMIL), Italy
The Coordinator

Hospital Environment Pilot (UPAT), Greece

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Cyprus University of Technology

Cyprus University of Technology (CUT), Cyprus

Panepistimiako Geniko Nosokomeio Irakleiou (PAGNI), Greece

www.pagni.gr
Πα.Γ.Ν.Η.

AEGIS IT RESEARCH

Aegis IT Research GMBH (AEGIS), Germany

SPHYNX Analytics Limited (SPHYNX), Cyprus

Sphynx Analytics

Ethical AI Novelties (EAIN), Cyprus

Trinomial Technologies (TRID), Cyprus

Trinomial
Research. Development. Innovation

LIBRA
A.I. Technologies

Libra AI Technologies (LIBRA), Cyprus

AERAS has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 872735.

AERAS

AERAS

Meet the AERAS Secondees

Efstratios Syrmas

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ UNIVERSITY OF PATRAS → Trinomial Research. Development. Innovation

Find out more about Efstratios on LinkedIn

www.linkedin.com/in/stratos-syrmas-0a817a228

I'm Efstratios Syrmas, a PhD Candidate at the University of Patras, and I had the incredible opportunity to complete a secondment at Trinomial Technologies Ltd from May 9 to October 8, 2024, as part of the AERAS project. This experience allowed me to apply my academic knowledge in a real-world setting, working on cybersecurity, platform integration, and user experience enhancement within the healthcare sector.

During my secondment, I contributed to Work Package 4 (WP4) and Work Package 5 (WP5), focusing on platform development, integration, and validation. My work played a key role in two major deliverables:

› D4.4 - AERAS Monitoring, Assessment, and Adaptation Mechanisms – V2

To ensure the AERAS platform remained effective and adaptable, I helped design an Evaluation and Adaptation checklist. This structured framework allowed for regular assessment of the platform's impact and training modules, ensuring ongoing improvements based on real-world feedback. The iterative approach we implemented made it possible to refine the AERAS methodology and enhance the training experience for participants.

› D5.4 - Final Prototype of Integrated AERAS Platform

As part of the effort to deliver a fully functional and user-friendly platform, I worked on optimizing the User Interface (UI), making it more intuitive and accessible for end-users. My focus was on streamlining the experience so that users could easily navigate and engage with the platform's features.

Additionally, I developed a specialized questionnaire aimed at uncovering cybersecurity risks in hospital environments. This tool was designed to identify vulnerabilities and strengthen the security framework of the AERAS pilots, ensuring that the platform could address real-world cybersecurity challenges in medical settings.

This experience at Trinomial Technologies Ltd was invaluable for me, as it allowed me to bridge the gap between research and industry. I was able to see first-hand how theoretical concepts translate into practical solutions, particularly in the critical field of cybersecurity for healthcare.

Beyond the technical aspects, the secondment also helped me develop new problem-solving skills, collaborate with industry experts, and gain a deeper understanding of real-world cybersecurity challenges. The collaboration between University of Patras and Trinomial Technologies also reinforced the importance of knowledge exchange between academia and industry.

Looking back, I can confidently say that this secondment broadened my perspective and significantly contributed to my professional growth. It was an exciting and fulfilling experience that strengthened my expertise and prepared me for future challenges in the field.

AERAS

Meet the AERAS Secondees

Ioana Stamoulli

My name is Ioanna Stamouli, and I am a PhD student at the University of Patras. My academic journey began with a degree in Physics at the Aristotle University of Thessaloniki, followed by an MSc in Medical Physics at the University of Patras. As part of my research and professional development, I had the opportunity to complete a secondment at Trinomial Technologies Ltd from May 9, 2024, to October 8, 2024, within the framework of the AERAS project.

During my time at Trinomial, I worked on Work Package 4 (WP4) and Work Package 5 (WP5), specifically contributing to two major deliverables:

- **D4.4 - AERAS Monitoring, Assessment, and Adaptation Mechanisms – V2**

A major focus of my work was the Evaluation and Adaptation checklist, a structured, iterative framework designed to continuously assess the effectiveness of the AERAS platform and its training modules. This checklist allowed us to gather feedback, analyze performance, and refine the approach to ensure the platform met the needs of trainees. By implementing this systematic evaluation process, we helped enhance the impact and sustainability of AERAS training activities.

- **D5.4 - Final Prototype of Integrated AERAS Platform**

Collaborating with my colleagues at Trinomial, I worked on the AERAS platform's User Interface (UI), focusing on creating an intuitive and user-friendly web application. The platform serves as the central access point for end-users, allowing them to interact seamlessly with the AERAS micro-services. My contributions were particularly centered around integrating user management features and developing interactive components that enhance the trainees' experience, making the platform more accessible and functional.

This secondment at Trinomial Technologies Ltd was an eye-opening experience that allowed me to apply my academic background in medical physics to a technological and cybersecurity-focused environment. Working alongside industry professionals gave me invaluable insights into real-world software development, platform integration, and user experience design.

Beyond the technical skills, this experience taught me the importance of interdisciplinary collaboration—bringing together expertise from physics, medical sciences, and IT to create a solution that benefits healthcare professionals and trainees.

Reflecting on this journey, I can confidently say that my secondment at Trinomial not only enhanced my professional skill set but also provided a deeper understanding of the intersection between technology, security, and healthcare. It was a truly rewarding experience that strengthened my ability to bridge the gap between research and real-world application.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ UNIVERSITY OF PATRAS → Trinomial Research. Development. Innovation

Find out more about Ioanna on LinkedIn

https://www.linkedin.com/in/ioanna-stamouli/

AERAS

Meet the AERAS Secondees

Theodoros Christophides

As a Special Scientist C and Project Manager at the Network Systems and Science Research Laboratory (NetSySci) since 2015, I have been deeply involved in research and innovation in cybersecurity, network systems, and digital resilience. My passion for advancing cybersecurity education and training has driven my work, both in academia and in real-world applications.

Currently, I am pursuing a PhD at Cyprus University of Technology (CUT) in the Department of Electrical Engineering, Computer Engineering, and Informatics, where I focus on cybersecurity training methodologies and system evaluation. My research aims to bridge cutting-edge academic theories with practical applications, ensuring that cybersecurity strategies evolve to meet modern threats effectively.

As part of my secondment to PAGNI from July 3, 2024, to September 2, 2024, under WP4: Key Components Development and Task 4.3, I have been working on real-time trainee assessment systems and Cyber Range program evaluations. This experience has allowed me to enhance cybersecurity training methodologies, develop innovative assessment tools, and refine cyber defense simulation environments to improve the effectiveness of cybersecurity education.

Through my work, I strive to contribute to the development of more robust cybersecurity infrastructures by integrating research-driven solutions into practical training programs. I am committed to ensuring that cybersecurity professionals are equipped with the skills and knowledge needed to navigate today's digital threats, ultimately strengthening digital resilience at both organizational and national levels.

Find out more about Theodoros on 🔗

https://netsysci.cut.ac.cy/theodoros.christophides/

Cyprus University of Technology → Πα.Γ.Ν.Η. www.pagni.gr

AERAS

Meet the AERAS Secondees

I am Loukas Papadoulas, Managing Director at Ethical AI Novelties Ltd, specializing in web-scale data science and machine learning. With over 20 years of experience in both technical and managerial roles, I have spent the last four years leading AI Cyprus Ethical Novelties Ltd and more than seven years implementing research grants.
From August 1, 2024, to May 31, 2025, I was a secondee at LIBRA AI in Athens, Greece, where I contributed to Work Package 3 (WP3), specifically Task 3.3 and Deliverable D3.3. This secondment provided an exciting opportunity to apply advanced data science techniques to cybersecurity training, reinforcing the AERAS project's commitment to AI-driven security solutions.

In my role, I led the development of a comprehensive data pipeline designed to:
› Harvest vulnerability data from online cybersecurity databases, ensuring a continuous stream of up-to-date and relevant security threats.
› Process and analyze vulnerabilities to detect critical weaknesses in infrastructure, providing valuable insights into emerging cybersecurity risks.
› Leverage language models to generate realistic training scenarios based on the extracted vulnerabilities, enabling AI-enhanced cybersecurity training that reflects real-world threats.
This structured pipeline **(see next page for more details for the pipeline)** serves as a foundational component for automated, scalable cybersecurity training, offering a data-driven approach to identifying, analyzing, and mitigating cyber risks.

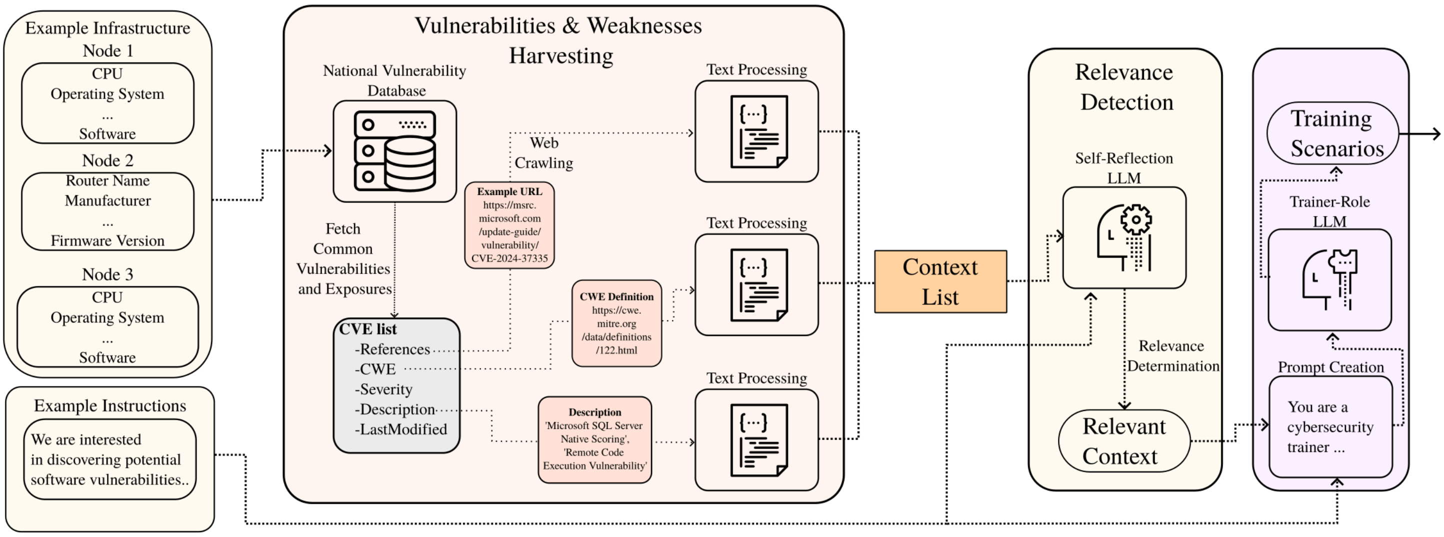
Loukas Papadoulas

LIBRA
A.I. Technologies

Find out more about Lukas on LinkedIn

change this link

Working at LIBRA AI broadened my perspective on the integration of AI and cybersecurity, particularly in the practical application of language models for security training. The opportunity to lead high-impact research while collaborating with experts in AI-driven security solutions allowed me to enhance my technical expertise and managerial leadership.
This secondment also strengthened cross-industry collaboration between research institutions and AI-driven enterprises, reinforcing the importance of interdisciplinary approaches in tackling cybersecurity challenges.
Reflecting on my experience, I can confidently say that this secondment at LIBRA AI was a strategic milestone in my career, enabling me to drive innovation at the intersection of AI, data science, and cybersecurity.


Example Infrastructure
Node 1
CPU
Operating System
...
Software
Node 2
Router Name
Manufacturer
...
Firmware Version
Node 3
CPU
Operating System
...
Software
Example Instructions
We are interested in discovering potential software vulnerabilities..
Vulnerabilities & Weaknesses Harvesting
National Vulnerability Database
Fetch Common Vulnerabilities and Exposures
CVE list
-References
-CWE
-Severity
-Description
-LastModified
Web Crawling
Example URL https://msrc. microsoft.com /update-guide/ vulnerability/ CVE-2024-37335
CWE Definition https://cwe. mitre.org /data/definitions /122.html
Description 'Microsoft SQL Server Native Scoring', 'Remote Code Execution Vulnerability'
Text Processing
Text Processing
Text Processing
Context List
Relevance Detection
Self-Reflection LLM
Relevance Determination
Relevant Context
Training Scenarios
Trainer-Role LLM
Prompt Creation
You are a cybersecurity trainer ...

Enhancing Cybersecurity Training Through AI-Driven Vulnerability Analysis

As part of the AERAS deliverable D3.3, an advanced cybersecurity pipeline has been developed to automate the process of identifying vulnerabilities and transforming them into realistic training scenarios. This innovative approach integrates machine learning, web crawling, and natural language processing to create tailored cybersecurity exercises, ensuring that professionals are trained on the most relevant and emerging threats.

From Data to Actionable Training: How the Pipeline Works

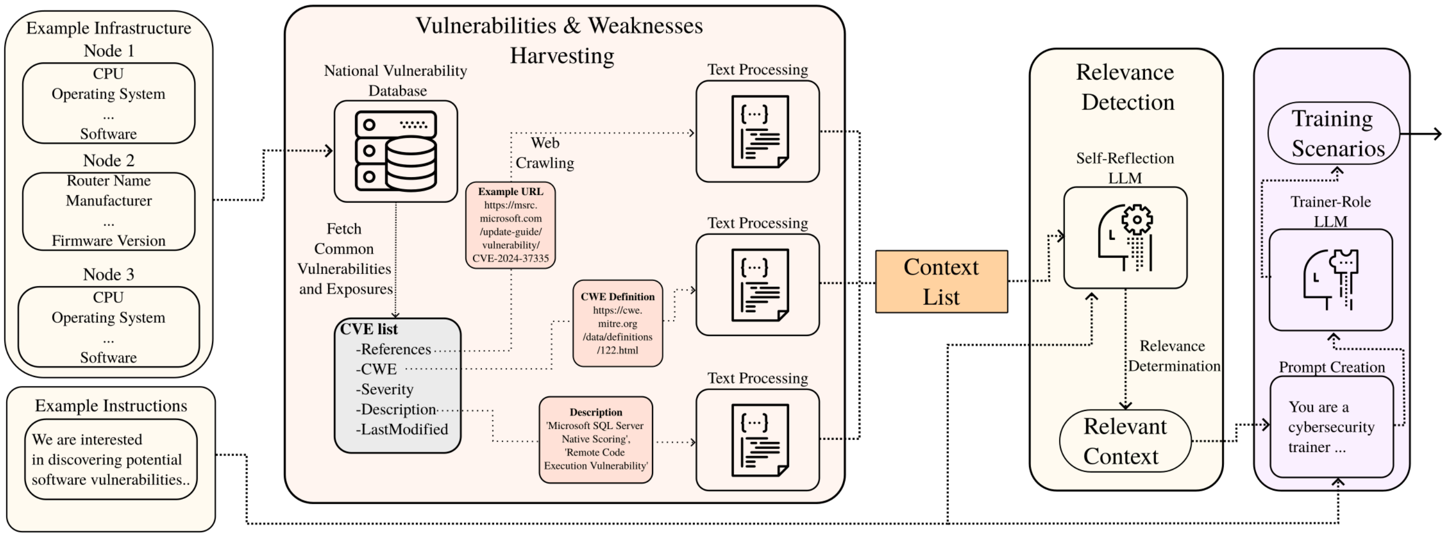
This pipeline integrates multiple stages, including data gathering, natural language processing, relevance detection, and prompt-based scenario generation. It leverages deep learning models to ensure that the training scenarios are closely aligned with real-world cybersecurity threats pertinent to AERAS pilot infrastructure. Next we present an extensive breakdown of each stage:

1. Example Infrastructure

> **Nodes:** This stage represents an example infrastructure setup with various nodes (e.g., Node 1, Node 2, Node 3), where each node contains specific hardware and software information, such as CPU, operating system, router name, manufacturer, firmware version, etc.
> **Instructions:** The infrastructure also includes example instructions indicating a focus on identifying potential software vulnerabilities. The goal is to find and prioritize software weaknesses that could pose security risks.

2. Vulnerabilities & Weaknesses Harvesting

> **Data Sources:** This section includes a connection to a "National Vulnerability Database" or a similar repository, which would be a collection of known security vulnerabilities (like CVEs — Common Vulnerabilities and Exposures).
> **Web Crawling:** The system uses web crawling to gather data from relevant sources. URLs, CVE references, CWE (Common Weakness Enumeration) definitions, descriptions, and severity scores are gathered for each identified vulnerability.
> **CVE List:** For each vulnerability, relevant information is collected, including:
References: Links or references to the vulnerability’s documentation.
CWE (Common Weakness Enumeration): This provides a classification of the type of weakness.
> **Severity:** A risk score that helps prioritize the vulnerability.
> **Description:** A summary of what the vulnerability entails, like "Remote Code Execution Vulnerability."
> **LastModified:** This tracks the most recent updates, ensuring you’re working with current information.
>**Text Processing:** Collected text data, including descriptions and references, goes through a text processing phase. This step likely involves cleaning, structuring, and preparing the data for relevance analysis.



Enhancing Cybersecurity Training Through AI-Driven Vulnerability Analysis

3. Relevance Detection

> **Context List:** The processed information is organized into a "Context List," which acts as a curated collection of vulnerabilities and weaknesses. This list will be evaluated to determine which items are relevant to your infrastructure and objectives.
> **Self-Reflection LLM:** A language model (LLM) with a self-reflective mechanism is used for "Relevance Detection." This step likely involves the model analyzing the context list and comparing it to the infrastructure details to identify relevant vulnerabilities.
> **Relevance Determination:** The LLM filters or prioritizes items based on their relevance to the infrastructure, potentially guided by specific criteria or thresholds for what is considered a high-risk or relevant vulnerability. The result of this process is the "Relevant Context," a refined subset of the original context list focused on critical vulnerabilities.

4. Training Scenarios

> **Prompt Creation:** Once the relevant context has been identified, prompts are created to guide a separate trainer-role LLM. These prompts set the scene for cybersecurity training scenarios, tailoring them to the vulnerabilities and weaknesses identified earlier.
> **Trainer-Role LLM:** The trainer-role LLM uses these prompts to generate training scenarios, acting as a "cybersecurity trainer." This LLM is responsible for creating realistic and specific training exercises, which could involve simulating attacks, defenses, or mitigation strategies based on the discovered vulnerabilities.
> **Output - Training Scenarios:** The final output consists of tailored training scenarios that can be used to train cybersecurity teams or develop countermeasures for the vulnerabilities identified in the infrastructure. These scenarios are designed to enhance the preparedness and responsiveness of cybersecurity professionals.

by Loukas Papadoulas,
Ethical AI Novelties

AERAS

Follow us for our latest news

You can see more about the project on our website:

https://www.aeras-project.eu/

@aeras.eu.H2020
https://www.facebook.com/aeras.eu.H2020

@aeras-eu
https://www.linkedin.com/company/aeras-eu/

@EuAeras
https://twitter.com/EuAeras

UNIVERSITÀ DEGLI STUDI DI MILANO

AEGIS IT RESEARCH

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ UNIVERSITY OF PATRAS

Trinomial Research. Development. Innovation

AI CYPRUS ETHICAL NOVELTIES LTD.

Sphynx Analytics

Cyprus University of Technology

LIBRA A.I. Technologies

www.pagni.gr Πα.Γ.Ν.Η.

AERAS has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 872735.

AERAS