



## Cloud-based Platform-agnostic Adversarial AI Defence framework- CPAID

### Welcome to the first Newsletter of cPAID!

cPAID is an EU-funded project shaping the future of trustworthy AI. cPAID aims to design, develop, and demonstrate a secure, transparent and accountable platform for AI-based services.

In this newsletter, we proudly present a recap of our achievements as well as what is coming up! Enjoy and don't forget to follow us online.



Funded by  
the European Union



The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

# Objectives

- ✓ **Objective 1:**  
Develop a Platform for holistic protection and robustness enhancement of AI systems
- ✓ **Objective 2:**  
A MLPrivSecOps methodology enhancing the traditional MLOps using Generative Adversarial AI and Context Awareness methods.
- ✓ **Objective 3:**  
A ML-driven risk management ontology tailored to the needs of AI systems.
- ✓ **Objective 4:**  
An AI-assisted Adversarial Intrusion Detection and Prevention system.
- ✓ **Objective 5:**  
Creation of cyber ranges for adversarial attacks to raise awareness, enhance the knowledge of AI professionals.
- ✓ **Objective 6:**  
Deployment, validation and evaluation in real-life use-cases.
- ✓ **Objective 7:**  
Communication and dissemination of cPAID results in maximizing its impact.



Funded by  
the European Union



The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

# Pilots

## Pilot 1

Monitoring the batteries of Electric Vehicles via worker robots. This pilot uses AI-enabled worker robots to monitor electric vehicle batteries in real-time. cPAID enhances the system's resilience against cyber threats, ensuring secure and uninterrupted battery diagnostics.

## Pilot 2

Monitoring of wild forests with 5G drones and their charging stations. AI-powered drones with 5G connectivity scan forests to detect early signs of wildfires. cPAID safeguards communication and AI analysis pipelines from potential attacks or failures. The result is a more reliable and rapid wildfire detection and response system.

## Pilot 3

Monitoring of remote AI-assisted medical devices. This pilot secures the operation of AI-based medical devices used in remote health monitoring. cPAID introduces robust mechanisms to defend sensitive systems against adversarial threats. It ensures patient data protection and sustained trust in digital healthcare.

## Pilot 4

Securing the AI systems of autonomous ships. AI is used for navigation and safety aboard autonomous vessels in this pilot. cPAID provides protection against manipulation and ensures the reliability of AI-driven decisions. It contributes to safe and secure autonomous maritime operations.

## Pilot 5

Security Training for experts. This pilot delivers hands-on training on securing AI systems through immersive simulation environments. cPAID integrates real-world adversarial scenarios and validation techniques into the training. It helps develop advanced capabilities for the next generation of cybersecurity professionals.

[For more information click here](#)



Funded by  
the European Union



The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

# Events

## BEYOND Expo, Athens / Greece



As coordinator of the EU-funded project CPAID, Uni Systems was proud to participate in the BEYOND Expo, held from April 4–6 in Athens.

For three dynamic days, we engaged in meaningful discussions, explored cutting-edge ideas, and connected with visionary experts across the tech ecosystem. CPAID drew the attention of more than 30 stakeholders from the ICT sector, thanks to its innovative approach to the holistic protection of AI applications against malicious activities and adversarial attacks.

Our team highlighted real-world challenges and shared ideas on certifying robustness, security, privacy, and ethical excellence of AI applications. The event offered a valuable platform to present CPAID's vision and objectives, raise awareness, and gather insightful feedback from a diverse audience.

We're excited about the new opportunities and potential collaborations that emerged during BEYOND and look forward to what comes next!"



Funded by  
the European Union

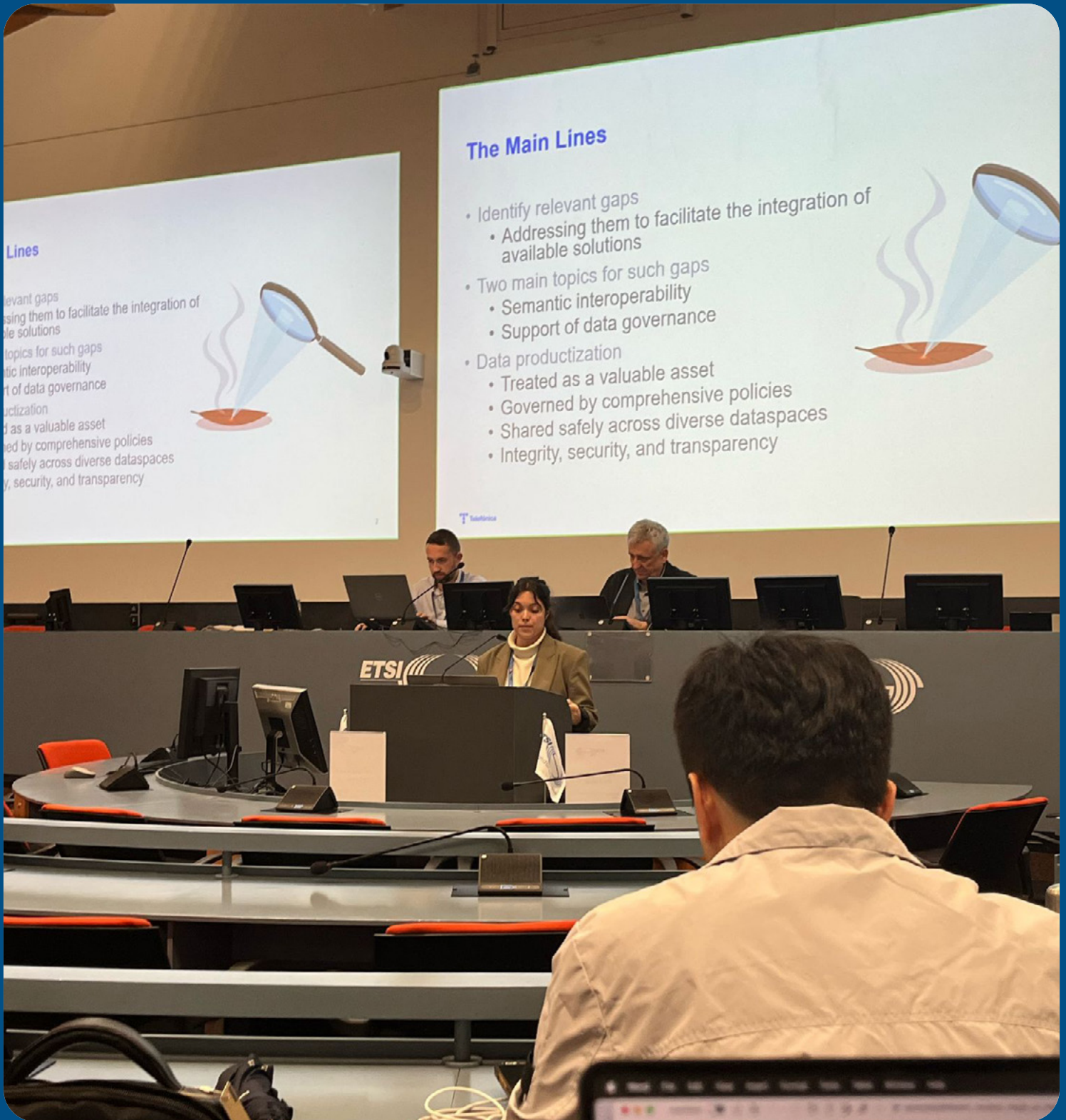


ECCC  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

# Events

## ETSI TC DATA Kick-off Sophia-Antipolis / France



[See all events here](#)



Funded by  
the European Union



The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

# Future events

ARES 2025 Ghent/Belgium 11-14 August 2025



# ARES

## conference

Availability • Reliability • Security

NEXUS 2025 Luxembourg 17-18 June 2025



# \*NEXUS

Luxembourg

2025

Accelerating AI & Tech  
for a Better Tomorrow

June 17 – 18, 2025

Luxembourg City

[See all events here](#)



Funded by  
the European Union

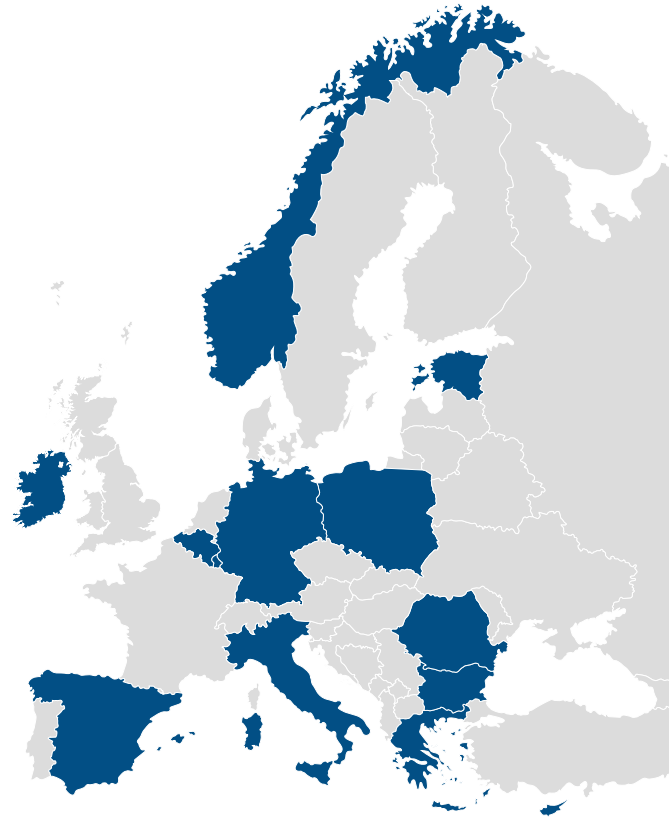


The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.



# The Consortium

The project unites 17 partners from 11 countries:  
Luxembourg, Greece, Romania,  
Poland, Cyprus, Spain, Estonia,  
Germany, Belgium, Ireland, Norway,  
Italy, Bulgaria



## Follow Us

Scan for more



Funded by  
the European Union



The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.