



Cloud-based Platform-agnostic Adversarial AI Defence framework

Welcome to the second Newsletter of cPAID

From Foundations to Integration: cPAID Enters Its Next Phase

Over the past months, the cPAID project has progressed through an intensive phase of coordination, design consolidation, and alignment across its technical work packages and pilot use cases. This work has focused on strengthening the project's architectural foundations and establishing a shared understanding of objectives, interfaces, and responsibilities across the consortium. During this period, priority was given to internal collaboration and structured planning. These efforts are preparing the ground for upcoming integration, validation, and broader engagement activities.

This second newsletter presents a high-level snapshot of the project's current status, outlining design-level progress, preparation activities, and next steps, while maintaining a clear and transparent view of the project's maturity.



Photo cPAID 1st Plenary meeting, Braunschweig, Germany



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.

Progress Overview

During the reporting period, the cPAID consortium focused on consolidating the project's foundations and preparing for the next phases of work. Key activities included:

- **Technical alignment and coordination** across work packages to ensure a shared understanding of objectives, roles, and interfaces.
- **Design definition and specification** of core technical concepts, including AI risk management approaches, security monitoring architectures, and AI-assisted defence mechanisms.
- **Clarification of component interfaces** to support future integration and interoperability within the cPAID framework.
- **Pilot preparation and use-case alignment**, ensuring that technical designs remain closely connected to real-world operational scenarios.
- **Maturation of dissemination and communication processes**, with core channels and tools in place to support future outreach and engagement.
- **Synergies with two EU-funded projects under the same call (GuardAI, CoEvolution)**, the first joint meeting has been held and proved to be very fruitful. Both projects have been invited to present their work at the upcoming Plenary Meeting.

Overall, this period marks a **transition phase** for the project, finalizing first versions of Cpaid components, moving toward structured integration, validation, and increased external engagement in the upcoming stages.



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.

Technical Work – Design & Foundations

During this period, technical work within cPAID focused on **coordinating, discussing, and refining design concepts across core components, reflecting the project's iterative, alignment-driven approach**. Key activities included:

✓ Risk Management for AI (RIMA)

- Ongoing refinement of the **overall AI risk management approach**.
- Clarification of conceptual roles and interactions between risk assessment, evidence sources, and alerting.
- Continued consideration of AI governance and trustworthiness aspects.

✓ Meta-SIEM (mSIEM)

- Continued **architectural discussion and design clarification** of the mSIEM concept.
- Refinement of core functional elements, including correlation logic, explainability, and operator interaction.
- Progressive alignment with other components and pilot requirements.

✓ AI-assisted Security Modules

- Conceptual discussion of AI-assisted security mechanisms, including penetration testing, vulnerability analysis, and human-factor considerations.
- Clarification of how these elements may provide evidence for monitoring and risk assessment.

✓ Data Fabric and Integration Considerations

- Coordination on data exchange principles and interface expectations.
- Discussion of integration needs across heterogeneous pilot environments.
- Alignment with platform-level and data-governance activities.

✓ MLPrivSecOps

- Ongoing definition of the **MLPrivSecOps approach**, focusing on the integration of privacy and security considerations across the machine learning lifecycle.
- Discussion of how ML development, deployment, and monitoring activities can incorporate risk-aware and privacy-preserving practices.
- Alignment with AI risk management, monitoring, and data governance concepts within the cPAID architecture.

✓ Generative Adversarial AI (GenAAI)

- Conceptual definition of **Generative Adversarial AI mechanisms** for simulating adversarial behaviors against AI systems.
- Exploration of how generative techniques can support robustness assessment, stress testing, and adversarial scenario generation.
- Alignment of GenAAI outputs with AI risk assessment and security monitoring components.

Overall, this phase focused on **iterative design and coordination**, establishing a shared understanding across partners while preparing for subsequent implementation and integration activities.



Pilot Preparation & Use-Case Alignment

During this period, work related to the pilots focused on preparation, coordination, and alignment activities, ensuring consistency between technical concepts and real-world use-case needs. Key aspects included:



Clarification of pilot scope and objectives, based on ongoing discussions with pilot owners and technical partners.

Alignment between pilot requirements and technical design concepts, supporting realistic expectations for future integration activities.

Identification of pilot-specific constraints and dependencies, including operational, technical, and data-related considerations.

Coordination across work packages to ensure that pilot use cases remain consistent with evolving architectural and design discussions.

Overall, these activities supported a shared understanding of pilot expectations and readiness, laying the groundwork for integration and validation as the project progresses.



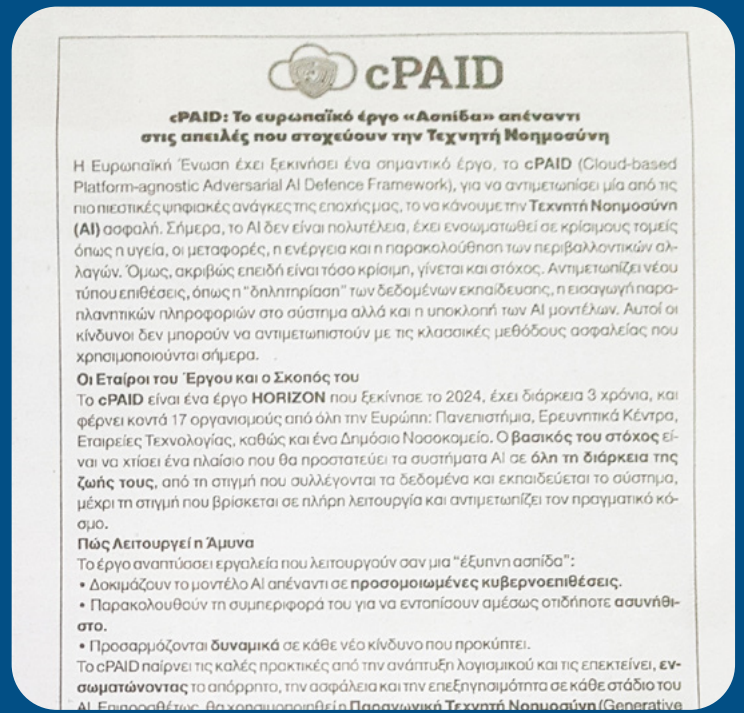
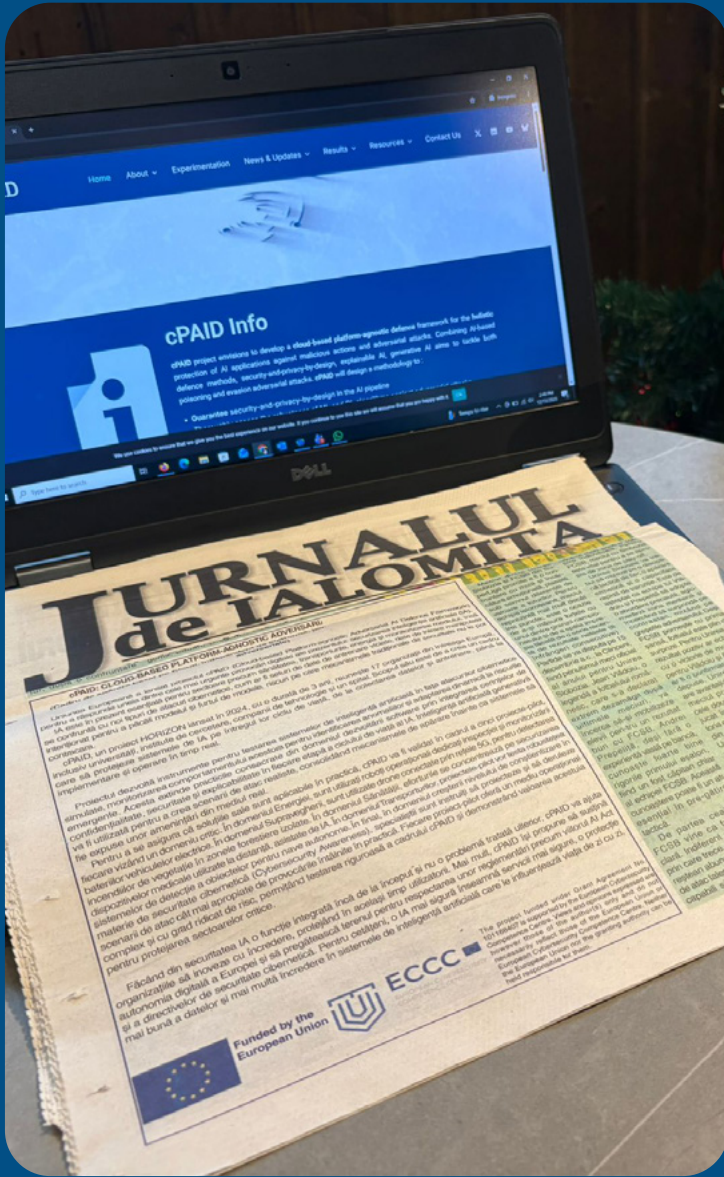
Funded by
the European Union



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.

cPAID in Traditional Media



During this period, the cPAID project was featured in **traditional media outlets in Luxembourg, Greece and Romania**, contributing to wider public awareness of the project's objectives and its focus on trustworthy and secure AI systems.

The published articles presented cPAID in the context of **emerging challenges in AI security and resilience**, highlighting the importance of European research initiatives addressing adversarial AI threats and real-world use cases. These publications reflect growing interest in the project's vision and reinforce its relevance beyond the research community.

Events & Community Engagement

During the reporting period, cPAID was represented in a range of external events, including conferences, workshops, exhibitions, and webinars, supporting engagement with research, industry, and standardisation communities.

HMU / PASIPHAE Special Session: Cybersecurity for Yielding Protection in Hyperconnected Ecosystems and Resilience

cPAID supported a special session at **EEITE 2025**, where Hellenic Mediterranean University (HMU) contributed to discussions on cybersecurity, AI resilience, and trustworthy AI in hyperconnected environments.



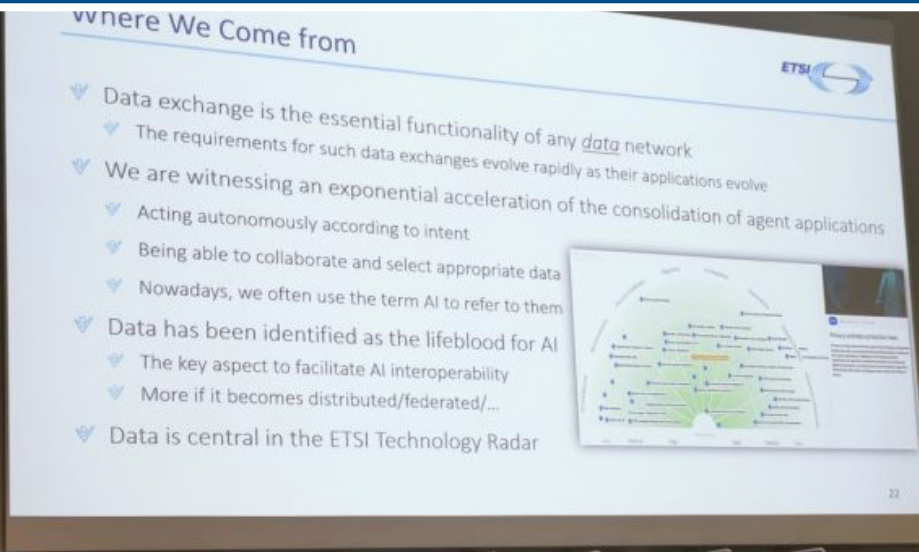
Technologies, Department of Digital Systems, University of Piraeus

AI in Financial Services 2025 Conference (Athens)

cPAID was represented at **AI in Financial Services 2025**, where **Prof. Christos Xenakis** highlighted key aspects of AI security and ethics in the financial sector.



Events & Community Engagement



6G FORGE

At the **6G FORGE** event, cPAID was represented by **Lucía Cabanillas (TELEFONICA)**, who contributed to discussions on future networks and AI security.



5th International Workshop on Advances on Privacy-Preserving Technologies and Solutions

cPAID was represented at the 5th International Workshop on Advances on **Privacy-Preserving Technologies and Solutions (IWAPS 2025)**, contributing to discussions on privacy, security, and trustworthy data processing in modern digital systems.



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 & Community Engagement



NEXUS – Luxembourg

cPAID was represented at **NEXUS 2025 in Luxembourg**, where Uni Systems presented the project and engaged with a broad international audience. The event provided an opportunity to discuss cPAID's approach to cybersecurity and trustworthy AI, with strong interest from public authorities and IT professionals exploring practical applications and real-world use cases.

2nd ASCI 2025 Conference (EST)

At the 2nd **ASCI 2025 Conference**, **CAFA Tech** represented cPAID in the Conference and Expo area, presenting the project's goals and vision to the autonomous systems community.



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 & Community Engagement

Hackathon Engagement – UNI.HACK 2025

cPAID supported **UNI.HACK 2025**, a hands-on hackathon focused on cybersecurity and AI challenges, bringing together students, researchers, and professionals to work on real-world problem scenarios. As part of the initiative, **INQBIT**, a member of the cPAID consortium, actively contributed to the event, supporting activities that promote responsible AI practices, adversarial AI awareness, and applied cybersecurity skills. Through its involvement, cPAID reinforced its commitment to capacity building and to connecting academic research with real-world cybersecurity and AI challenges. By supporting hackathons such as UNI.HACK 2025, cPAID encourages experiential learning and community-driven innovation, contributing to the development of the next generation of AI and cybersecurity experts.



cPAID Hosts the 1st CyberHammer Hackathon in Lisbon

On 24 January 2026, the cPAID project organised the **1st CyberHammer Hackathon in Lisbon**, alongside the **CSP Winter School**. The event brought together over 30 participants forming more than 12 teams, who worked intensively on 25 cybersecurity challenges across multiple domains.

The hackathon fostered hands-on learning, collaboration, and innovation, strengthening cybersecurity skills and community engagement. This successful first edition marks an important step in cPAID's commitment to capacity building and practical cybersecurity education.

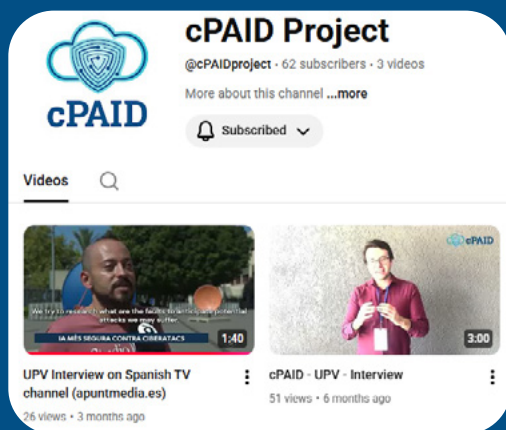


Video Interviews & Media Features

During this period, cPAID increased its visibility through video interviews, offering insights into the project’s objectives and its approach to trustworthy and secure AI systems.

An internal video interview was recorded to present cPAID’s vision, motivation, and key focus areas from within the consortium. In parallel, cPAID was featured in a video interview hosted by Spanish media outlet **À Punt Media**, highlighting the relevance of **European research efforts in AI security** and resilience to a wider public audience.

Both interviews are available on the [cPAID YouTube channel](#), supporting the project’s outreach by making complex cybersecurity and AI topics more accessible beyond the research community.



Future Events

March 2026 Athens, Greece DiGiTAL FiNANCE



Prof. Christos Xenakis

Jury President – Pillar #2: Digital Insurance

Director of the Master Course Digital Systems Security, Department of Digital Systems, University of Piraeus



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.