Newsletter Vol. 3

cPAID

Cloud-based Platform-agnostic Adversarial AI Defence framework

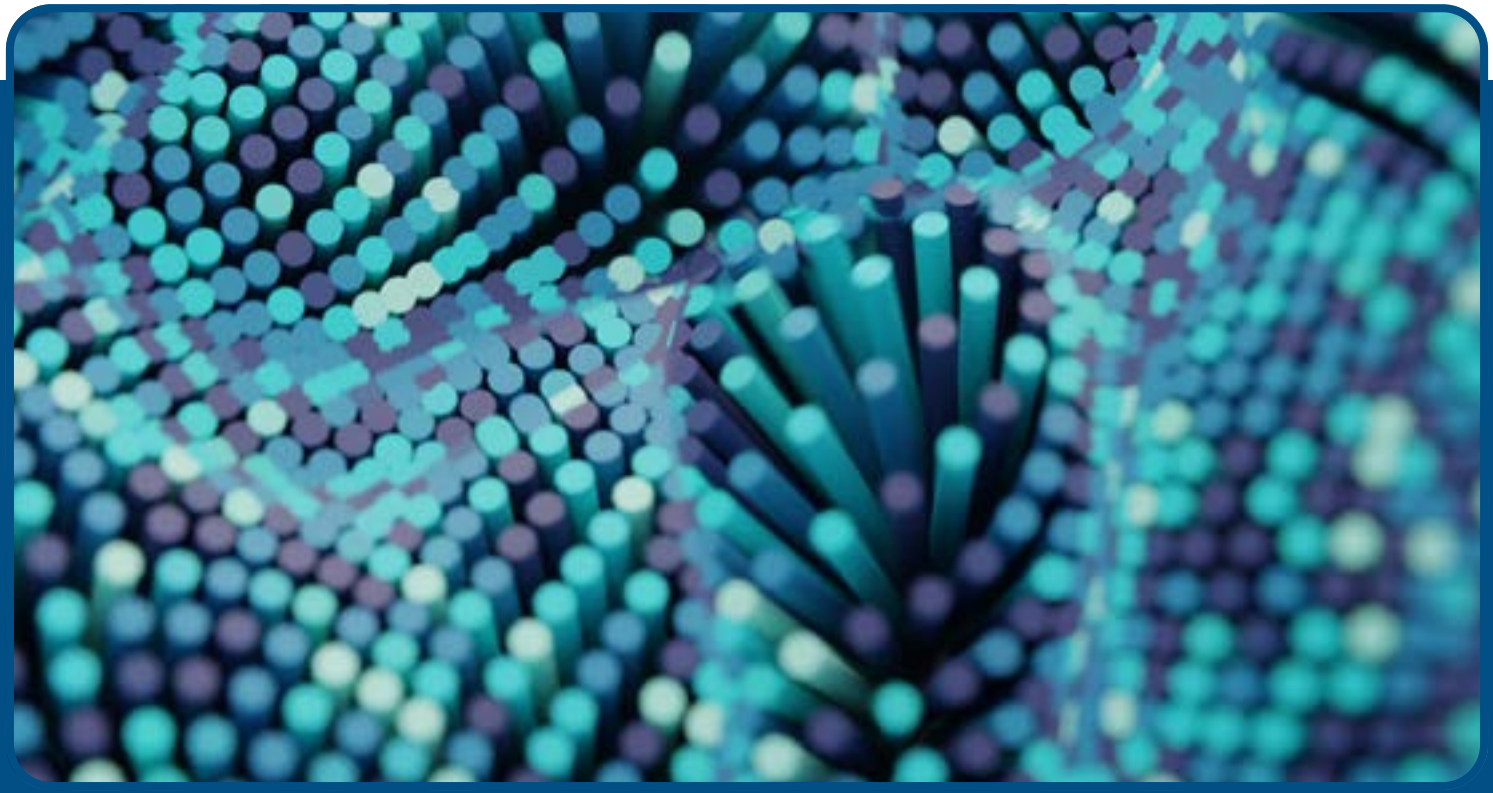
Welcome to the third Newsletter of cPAID!

From Integration Readiness to Pilot-Backed Impact

The cPAID project has successfully completed its first 18 months, marking an important transition from design consolidation to integration readiness.

During this period, the consortium delivered the initial architecture and first versions of the project's core components, including MLPrivSecOps, GenAAI, Data Fabric, RIMA, mSIEM and AIPS. These achievements establish a solid technological basis for the next phase of work, where integration, performance refinement and validation through real-life pilot environments become the central focus.

This third newsletter presents a high-level overview of the project's latest progress, including technical developments, pilot alignment, exploitation activities, standardisation engagement, scientific output and community outreach.



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.

Progress Overview

During the latest reporting period, the cPAID consortium moved from architectural planning and component-level design toward a more implementation-oriented phase.

Key highlights include:

- Delivery of the first versions of the cPAID core components, covering MLPrivSecOps, GenAAI, Data Fabric, RIMA, mSIEM, AIPS and the adversarial AI cyber range.
- Definition of 5 detailed pilot use cases and specific scenarios, supporting validation across diverse real-world environments.
- Consolidation of 107 requirements, including functional, non-functional, security, privacy, legal and ethical requirements.
- Progress toward an operational system-level architecture, with clearer component interconnections, data flows, control flows and adversarial-action flows.
- Establishment of the initial integration and validation framework, including pilot planning, KPI refinement and the first Red Team-Blue Team validation approach.
- Continued dissemination, exploitation and standardisation progress, supported by events, publications, media activity and growing engagement.

Overall, cPAID has entered a phase where technical outputs are increasingly connected to pilot needs, stakeholder expectations and future impact pathways.

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.

Technical Work

From Component Baselines to Integration Readiness

During this period, technical work focused on delivering and maturing first component versions, while preparing them for integration across the platform.

- **MLPrivSecOps**
  The first version of the methodology has been delivered, extending traditional MLOps with security, privacy and robustness-by-design principles.

- **GenAAI**
  The Attacker Knowledge Module has been implemented as a RAG-based microservice, producing structured outputs related to attack type, technique and parameters.

- **Data Fabric**
  The first architecture has been defined, together with a Data Registry for documenting data flows, datasets, formats, protocols and schemas.

- **mSIEM**
  The initial architecture and methodology have been defined, with monitoring, visualisation, alerting and incident-management capabilities under preparation.

- **RIMA, AIPS and Cyber Range**
  RIMA, AIPS and the adversarial AI cyber range have reached first operational baselines, supporting risk assessment, adversarial intrusion detection and hands-on training.

Together, these developments mark a shift from design-level preparation to early operational capability.

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.

Pilot Preparation & Use-Case Alignment

The five cPAID pilots remain central to the project's validation strategy. During the latest period, work focused on making pilot specifications more concrete, measurable and ready for deployment planning.

Pilot 1: Monitoring the batteries of Electric Vehicles via worker robots

Preparing AI-enabled monitoring and resilience mechanisms for electric vehicle battery diagnostics.

Pilot 2: Wild forest fire detection from drones

Supporting AI and 5G-enabled monitoring scenarios for early wildfire detection and secure drone-based data flows.

Pilot 3: Monitoring of remote AI-assisted medical devices

Strengthening cybersecurity and trust in connected medical-device environments.

Pilot 4: Securing the AI systems of autonomous ships

Using maritime data and simulation support to assess adversarial threats affecting autonomous maritime AI systems.

Pilot 5: Security training for experts

Providing practical adversarial AI training through cyber-range scenarios and hands-on exercises.

The next phase will focus on tool onboarding, pre-feasibility testing, KPI measurement and pilot-level validation.

Funded by the European Union

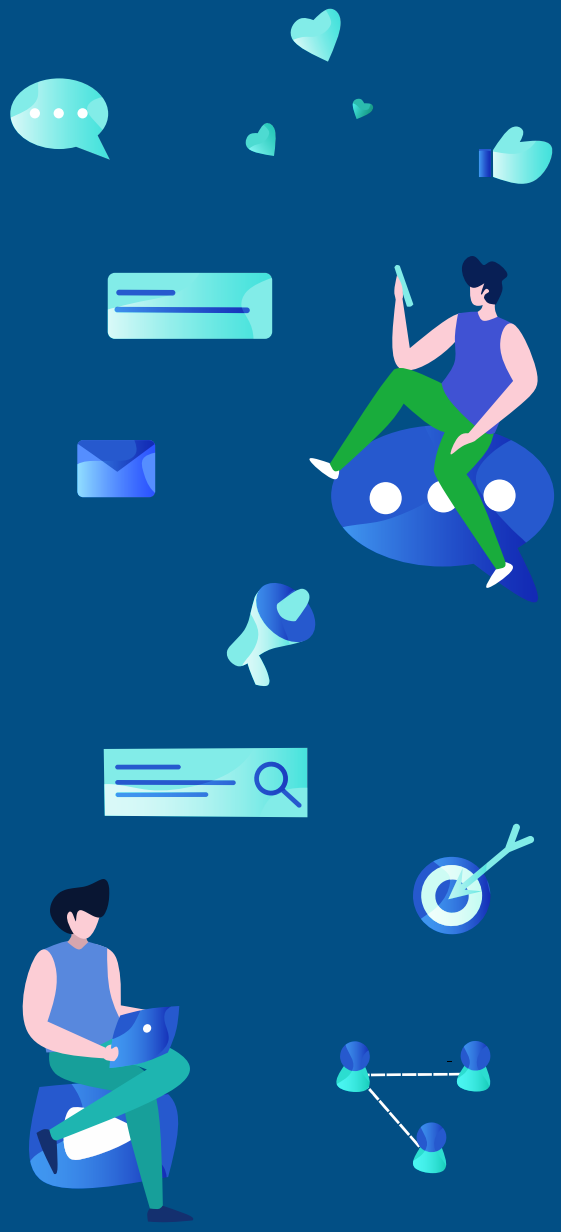
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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.

Dissemination & Communication Highlights

cPAID has continued to expand its visibility and engagement with research, industry and wider public audiences.

By M18, the project recorded:



2,900
unique website visitors

6,116
page views

379
followers across social media channels

16
recorded event participations.

1 **webinar and**
2 **sister-project synergies**

6
scientific publications captured in the KPI tracker

The website remains operational and updated with news, blogposts, publications, videos and newsletters. Communication materials have also been strengthened through a roll-up banner, flyers, a factsheet, videos and media features.

These activities support the project's outreach across technical and non-technical audiences.

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 & Community Engagement

cPAID continued to engage with relevant communities through conferences, workshops, exhibitions, hackathons and standardisation-oriented events.

Recent visibility and engagement activities include:

9th InsurTech Conference in Athens, January 2026.

Open Conf, Athens, November 2025

Mobile World Congress in Barcelona, March 2026

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 & Community Engagement

11th Ship IT Conference, Athens, September 2025

89th Thessaloniki International Fair, September 2025

Keynote at IEEE DESSERT, Athens, December 2025

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

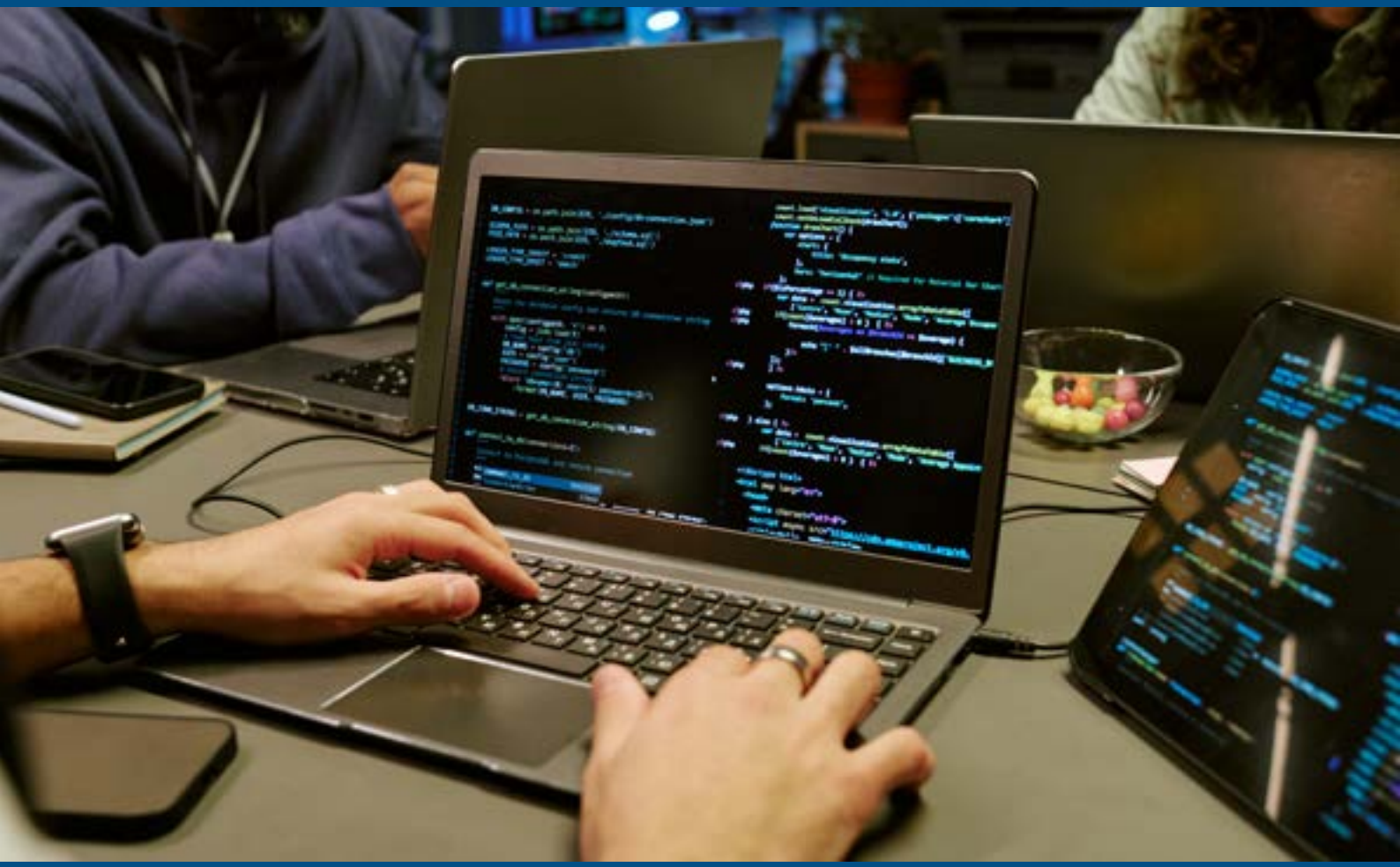
The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the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

Events & Community Engagement

Hackathon Highlights

The **2nd Hellenic University Hack** brought together **358 individuals**, **103 teams** and **16 universities**.

The **1st CyberHammer Hackathon**, held in conjunction with the CSP Winter School, involved **30 individuals**, **12 teams** and **24 challenges**.



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.

Exploitation - Building the cPAID Value Story

Although the main exploitation deliverables are scheduled for the final project stage, cPAID has already launched its exploitation workflow.

An Asset Identification Questionnaire was designed, distributed and consolidated across partner inputs, supporting the mapping of exploitable assets, TRLs, target markets, adopter needs, competitors and exploitation channels.

The emerging KER portfolio includes:

- **MLPrivSecOps Secure AI Lifecycle.**
- **GenAAI and AIPS adversarial AI defence capabilities.**
- **Data Fabric for interoperable and governed data exchange.**
- **mSIEM, Forensics Visualisation and response support.**
- **RIMA, AISocDog and AI-based harmonisation.**
- **PyGemini and validation/cyber-range assets.**

A first joint exploitation workshop introduced a bundle-based approach, helping partners translate individual assets into adopter-oriented value propositions.

Standardisation & Open-Source PathwaysStory

Standardisation and open-source engagement have become a strong area of progress for cPAID.
By M18, the project had tracked:

- **78 standardisation actions.**
- **Leadership in 2 committees.**
- **More than 10 documents.**
- **Engagement with more than 5 committees.**
- **8 open-source contributions.**

The standardisation pathway is led by TID and aligned with the project's technical outcomes. Activities focus on data governance, semantics, interoperability, and network and data management.

The project has actively positioned results around ETSI TC DATA, ETSI ISG ZSM and IETF/IRTF groups, including OPSAWG, NMOP, IVY and NMRG.

This work helps connect cPAID research outputs with broader technical communities and future uptake pathways.

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.

Looking Ahead

The next phase of cPAID will focus on turning RP1 achievements into integrated demonstrations and pilot-backed evidence.

Planned activities include:

- **Continued website updates, articles, social media posts and newsletters.**
- **Stronger video and demo storytelling by M24.**
- **Further webinars, workshops and external events.**
- **Finalisation of exploitable asset profiles and joint exploitation bundles.**
- **Advancement of the market analysis and exploitation plan.**
- **Continued ETSI/IETF monitoring, TC DATA positioning and open-source engagement.**
- **Conversion of visibility and asset mapping into pilot-backed impact evidence during RP2.**

As cPAID moves forward, the project will continue working toward secure, interoperable and reliable AI solutions that help organisations understand, monitor and defend against adversarial AI threats.

Funded by the European Union

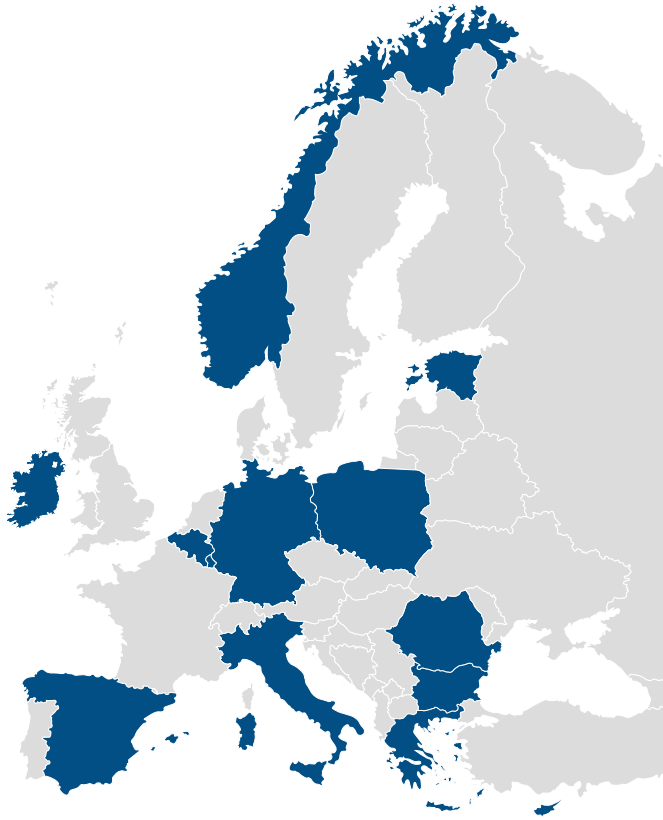
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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

The Consortium

cPAID unites 17 partners from 11 countries, bringing together research, industry, healthcare, telecom, cybersecurity, legal, maritime and technology expertise to advance trustworthy and resilient AI.



uni.systems

InQbit Innovations

orange

Suite5 We Deliver Intelligence

Universitat Politècnica de València

CAFA

Telefónica

AEGIS IT RESEARCH

VUB Vrije Universiteit Brussel

UBITECH ubiquitous solutions

konnektable TECHNOLOGIES

NTNU Norwegian University of Science and Technology

cnit consorzio nazionale interuniversitario per le telecomunicazioni

K3Y

Follow Us

www.cpaid.eu

/company/cpaid-project

/CpaidEUProject

/@cPAIDproject

Scan for more

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.