AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AIAS NEWSLETTER

Issue 5 | December 2025

AI systems find applications in various technical fields. However, their adoption exposes early users to vulnerabilities, such as data corruption, model theft, and adversarial samples. The lack of tactical and strategic capabilities to defend, identify, and respond to attacks on these AI-based systems is a significant concern. Adversaries exploit this vulnerability, creating a new attack surface that specifically targets Machine Learning and Deep Learning systems, posing a substantial threat to critical sectors like finance and healthcare. Addressing these challenges, the MSCA-funded AIAS project aims to conduct research on adversarial AI and develop an innovative security platform for organisations. This platform will employ adversarial AI defence methods, deception mechanisms, and explainable AI solutions to empower security teams, fortifying AI systems against potential attacks.

PROJECT COORDINATION
Prof. Christos Xenakis
School of Information and Communication Technologies
Department of Digital Systems
University of Piraeus
Karaoli and Dimitriou 80,PC 18534, Piraeus, Greece
Tel: +30 210 4142776
email: xenakis@unipi.gr

PROJECT DETAILS
Project number: 101131292
Project Website: aias-project.eu
Project start: 1st January 2024
Duration: 48 Months
Total cost: EUR 1564000
EC Contribution: EUR 1564000

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AIAS

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AIAS Objectives

- **Holistic Protection:** Conceptualize and develop a service architecture integrating AI-empowered applications, deception mechanisms, and mitigation techniques towards the holistic protection of organizations against cyberattacks and adversarial AI.
- **Attack Scenarios:** Design and develop a novel adversarial AI engine for creating attack scenarios tailored to the characteristics of the targeted organisations' hardware and software infrastructure.
- **Novel Intelligent Deception Methods:** Design and implement novel intelligent deception methods based on high-interaction honeypots, digital twins, and virtual personas.
- **AI-based Methods for Protection:** Design, develop, and assess AI-based methods for the detection and mitigation of cyberattacks including adversarial AI attacks as well as conceptualize and implement data collection and fusion methods.
- **XAI-based Recommendation Engine:** Develop and verify explainable AI (XAI)-based recommendation engine empowering human-in-the-loop proactive decisions to thoroughly mitigate adversarial AI attacks.
- **Real-life Usage:** Assess the functionality, effectiveness and efficiency of AIAS in real-life scenarios.

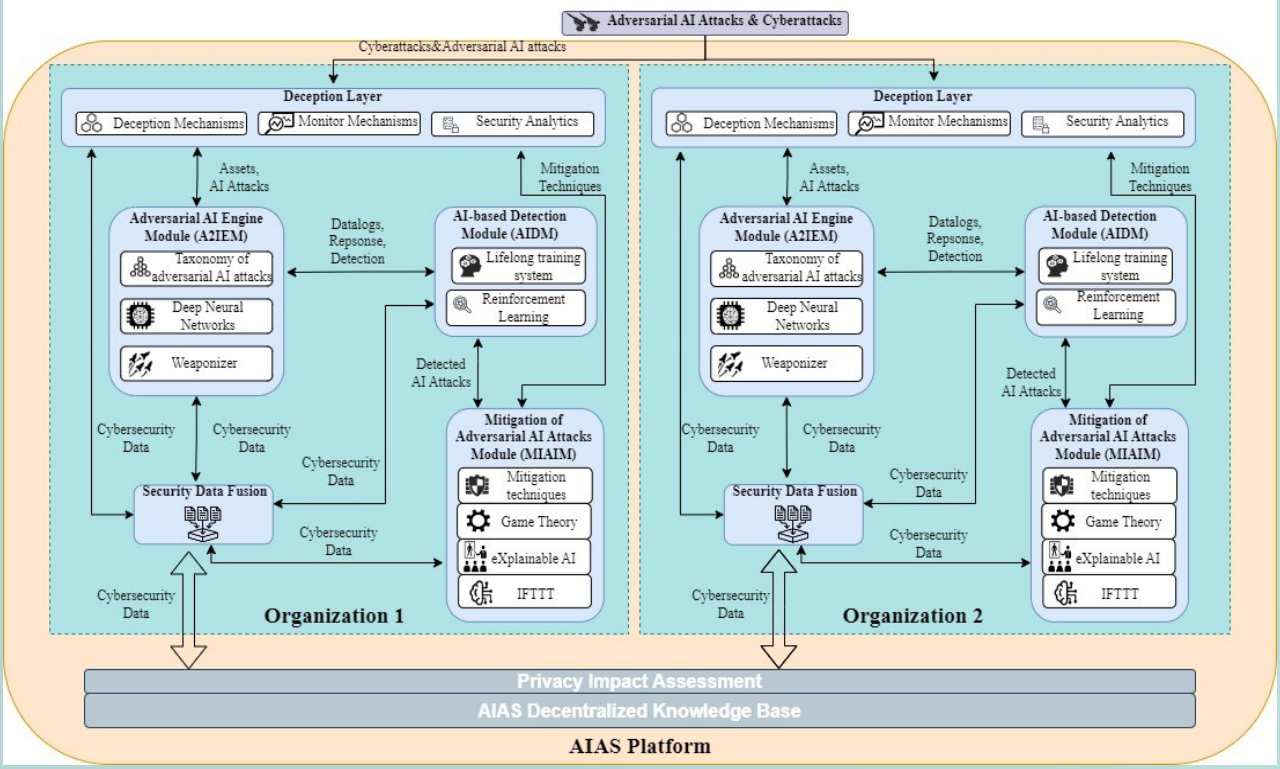
This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AIAS

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AIAS Architecture

- The AIAS architectural framework is constituted by an integrated set of components, each of which is designed to contribute to the formation of a unified cybersecurity defence system capable of safeguarding SMEs from sophisticated adversarial AI and cyber threats.
- The system comprises several key components, including the Adversarial AI Engine, the Deception Layer, the AI-based Detection Module, the XAI-based Mitigation Engine, and the Security Data Fusion and Decentralised Knowledge Base.



This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

News & Events

[Iman Hasnaouia Begins Secondment at K3Y!]

[Thank you Iman!]

[AIAS at IWAPS 2025!]

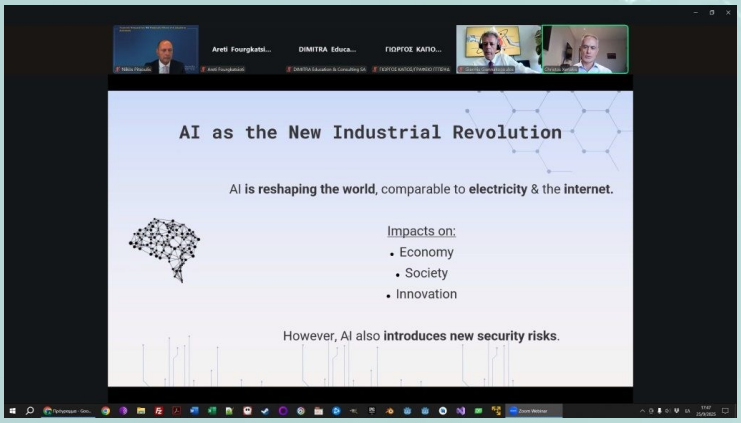
[AIAS Project at the 89th Thessaloniki International Fair!]

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

News & Events

[AIAS Project Supports Prof. Christos Xenakis in Advancing the Dialogue on AI and Digital Ethics in the Public Sector.]



[AIAS Featured in IEEE Study on Trust and AI for Consumer IoT Security!]

[Celebrating Researchers' Night in Athens!]

[AIAS Showcased at La Noche Europea de los Investigadores 2025 in Málaga!]

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

News & Events

New Publication in Array (Q1 Journal).

New Publication in PeerJ Computer Science!

AIAS Project Presented at U-MAkers: Advancing Trust and Privacy in the Digital AgeAnother event, another Milestone for AIAS.

The AIAS 2nd Brochure Is Now Available in Four Languages!

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AIAS Publication

- Ziras, G., Farao, A., Zarras, A., & Xenakis, C. (2025). From vulnerability to resilience: Adversarial training and real-time detection for AI security. Array, 100546.
- Zarras, A., Kollarou, A., Farao, A., Bountakas, P., & Xenakis, C. (2025). Testing the limits: exploring adversarial techniques in AI models.
- I. Politis, M. Bampatsikos, A. Zarras and C. Xenakis, "Trust Score Prediction for IoT Device Onboarding Using Transfer and Few-Shot Learning in Consumer Electronics," in IEEE Transactions on Consumer Electronics
- Kotsiopoulos, T., Radoglou-Grammatikis, P., Lekka, Z. et al. Defending industrial internet of things against Modbus/TCP threats: A combined AI-based detection and SDN-based mitigation solution. Int. J. Inf. Secur. 24, 157 (2025). https://doi.org/10.1007/s10207-025-01076-2
- Farao, A., Bolgouras, V., Zarras, A., & Xenakis, C. Cybersecurity Challenges and Pitfalls in 6G Networks.
- Petihakis, G., Farao, A., Bountakas, P., Sabazioti, A., Polley, J. and Xenakis, C., 2024, July. AIAS: AI-ASsisted cybersecurity platform to defend against adversarial AI attacks. In Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-7).

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AIAS

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

AIAS Publication

- Bampatsikos M, Politis I, Ioannidis T, Xenakis C. Trust Score Prediction and Management in IoT Ecosystems Using Markov Chains and MADM Techniques. IEEE Transactions on Consumer Electronics. 2025 Jan 17.
- Lacalle I, Cuñat S, Farao A, Xenakis C, Xenakis D, Palau CE. Deception Mechanisms for Cyber-Security Enhancement in the Internet of Things. In2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) 2024 Oct 21 (pp. 1-7). IEEE.

Upcoming Technical Deliverables

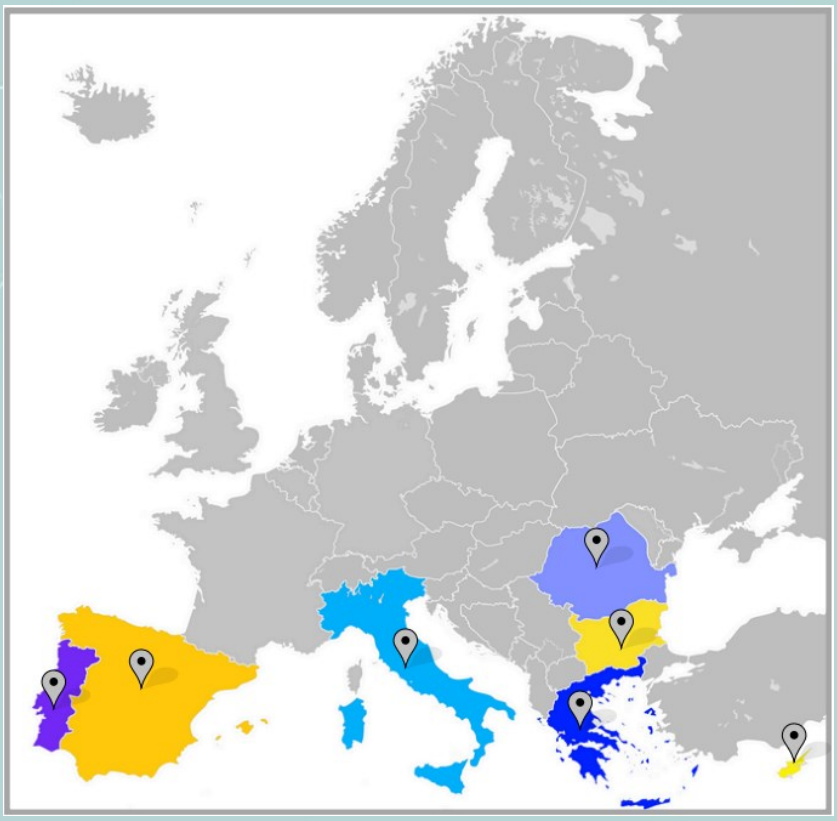
- D3.2-Taxonomy of AI Adversarial Attacks (December/2025)
- D3.3-Adversarial AI Engine (June/2026)
- D4.1-AI-based Detection of Adversarial AI Attacks (December/2026)

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.

AIAS

AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks

Meet the Consortium



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

cnit consorzio nazionale interuniversitario per le telecomunicazioni

UNIVERSIDAD DE MÁLAGA

K3Y R&D AND CYBER SECURITY

Beia CONSULT INTERNATIONAL

FOGUS INNOVATIONS & SERVICES

PDM

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Suite5 We Deliver Intelligence

Follow us for our latest news!

www.aias-project.eu

@AIAS.MSCA

@AIAS MSCA

@AIAS_MSCA

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292.