

ATTACK SCENARIOS



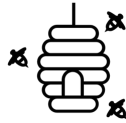
DT IoT Environmental monitoring platform for simulation and deception

An experimentation-oriented platform to evaluate threat scenarios within IoT ecosystems. Leveraging DTs, this approach assesses both simulation and deception for environmental monitoring systems with the aim of improving safety, reliability, and robustness of automated spaces.



VP-assisted DT for Healthcare leveraging AI-based anomaly detection

While DTs precisely mimic system behaviours, its combination with VP technologies allows for the simulation and reasoning based on stakeholders' perspective. Applied to healthcare scenario, VPs can contribute not only to decision-making, but also in the analysis of safety circumstances.



High Interaction Honeypot for Industrial Network protection

Defence against AI-driven threats under Modbus-based industrial networks considering both network and adversarial attacks. HIH and DTs deployed within the industrial infrastructure are leveraged for deception, while AIAS platform capitalises on the detection and mitigation of the attacks.



Protection of malware detection software against adversarial attacks

Identification and response to adversarial attacks on AI-based malware detection using the AIAS weaponizer tool. Through synthetic malware generation and AI-driven anomaly detection, adversarial attacks against the malware detection engine are detected.



Novel intelligent deception for SME services defence

Digital services are known to attract the interest of many adversarial AI attacks. This novel platform examines how attackers interact with SME systems, retrieving novel intelligence and attacks patterns that further enhance system's security.



AI-ASSISTED CYBERSECURITY PLATFORM

DECEMBER, 2025



HORIZON-MSCA-2022-SE-01-01;
HORIZON.1.2 - Marie Skłodowska-Curie Actions
(MSCA)

PROJECT WEBSITE: <https://www.aias-project.eu/>
PROJECT START: 1st January 2024
DURATION: 48 months
GRANT AGREEMENT: 101131292
EU CONTRIBUTION: EUR 1 564 000
COORDINATION: University of Piraeus Research Center (Greece)

NOVEL INTELLIGENT DECEPTION METHODS

AIAS project relies in cutting-edge deception solutions to assess threat intelligence:

Digital Twins (DT)

Digital replicas of physical assets that accurately mirror their behaviour in real-time, allowing for the study of the system and the identification of abnormal states that can compromise the system.

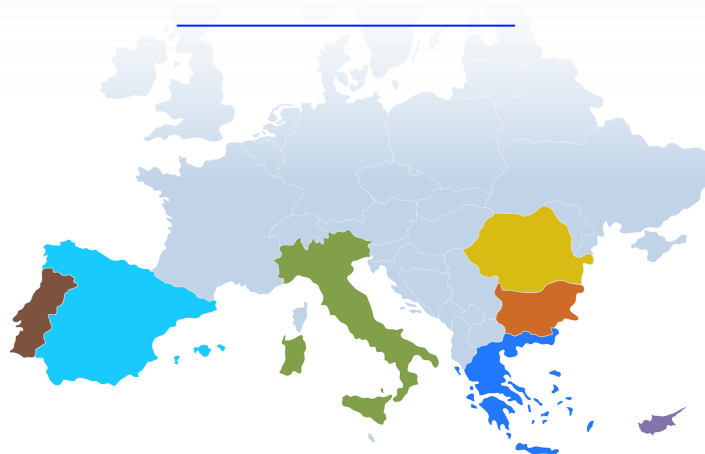
Virtual Personas (VP)

Digital representation of individual stakeholders of the system. They precisely mimic the interaction of real identities, responding to events in the system and providing an extra layer of realism in the production of virtual decoys.

High-Interaction Honeypots (HIH)

System implementations to create a false sensation of open vulnerabilities, offering a high degree of realism. While attackers concentrate their efforts on exploiting these features, the honeypot engage them to extract valuable insights regarding their actions and patterns. HIH not only extract intelligence from adversarial activity but also divert attackers away from critical components.

INTERNATIONAL COLLABORATION



METHODOLOGY

Phase 1: Definition of system requirements and platform's main components:

- Identify and define the requirements.
- SOTA reviews: Deception methods, AI-driven detection and Mitigation methods.
- Specify the tools and applications for each AIAS module implementation.

Phase 2: Implementation and validation of the main platform components:

- Deception Layer
- Adversarial AI engine Module
- Security Data Fusion
- AI-based Detection Module
- Mitigation of Adversarial AI Attacks Module

Phase 3: Integration, proof-of-concept study and real-life assessment.

For more information visit our website or follow us

