



AI4CYBER



LINKEDIN
AI4CYBER



X (TWITTER.COM)
@Ai4Cyber



YOUTUBE
AI4CYBER Project



OUR WEBSITE
<https://ai4cyber.eu/>



Trustworthy
artificial intelligence
for cyber security
reinforcement and
system resilience



Funded by the European Union (flag) This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.

In addition, we inform you of the possible processing of your social media data through the AI4CYBER profiles that TECNALIA keeps available on each social network in which it is present, all following the terms and conditions established in each social network.

AI4CYBER is a 3-year Horizon Europe project which started on 1 September 2022 with 12 partners. Artificial intelligence (AI) has lately proved to be a coin with two sides. On the one hand, it can be leveraged as a powerful defensive mechanism to improve system preparedness and response against cyber incidents and attacks, and on the other hand, it can be a formidable weapon attackers can use to damage, compromise or manipulate systems. AI4CYBER ambitions to provide an Ecosystem Framework of next-generation trustworthy cybersecurity services that leverage AI and Big Data technologies to support system developers and operators in effectively managing robustness, resilience, and dynamic response against advanced and AI-powered cyberattacks.



The ecosystem will be validated in three scenarios



Detection and mitigation of AI-powered attacks against the energy sector.

Objectives

- 1 **Deliver a new breed** of AI-driven software robustness and security testing services that significantly facilitates the testing experts work, through smarter flaw identification and code fixing automation.
- 2 **Provide cybersecurity services** for comprehension, detection and analysis of AI-powered attacks to prepare the critical systems to be resilient against them.
- 3 **Incident response support** by AI4CYBER will offload security operators from complex and tedious tasks offering them mechanisms to optimize the orchestration of the most appropriate combination of security protections, and continuously learn from system status and defences' efficiency.
- 4 **Ensure fundamental rights** and values-based AI technology in its services, through the integration of demonstrable explainability, fairness and technology robustness (security) capabilities in the AI4CYBER components.



Robustness and autonomous adaptation of **Banking applications** to face AI-powered attacks.



Resilient hospital services against advanced and AI-powered cyber-physical attacks.

AI4CYBER components



DE- TEC- TION

TES- TING

AI for Testing

AI4VULN

An open-source solution to automatic identification and **verification of vulnerabilities and weaknesses in the code** with much higher accuracy rate than existing vulnerability analysis solutions thanks to applying symbolic execution and the use of AI to support scalability.

AI4FIX

A fully open-source end-to-end vulnerability fixing solution supporting Java, **bringing automatic unit testing of proposed fixes**, which enables to shift the fixing of the vulnerability much earlier in the software development flow, which in turn saves development time and reworks.

AI for Prevention and Detection

AI4AICTI

An advanced solution that offers latest AI-powered Cyber Threat Intelligence (CTI) to **detection and threat simulation tools** for raising their efficiency, including data of both AML attacks and AI-boosted attacks.

AI4FIDS

A high-performance and accuracy detection solution for advanced and AI-powered attacks detection in distributed environments where **privacy of data processed by detection agents need to be kept**.

AI4SIM

An **Advanced cyberattacks simulation solution** capable to simulate advanced and AI-powered attacks against IT, OT and IoT systems depending on the customer needs.

AI4TRIAGE

AI-based root cause **analysis and alert triage** to prioritize events to focus on the response.

RES-
PONSE

AI for Response

AI4SOAR

AI-powered Security Orchestration, Automation and Response solution capable to deploy multiple security controls at different layers of the system for better react against cyber incidents and attacks.

AI4ADAPT

The service that will enrich the AI4SOAR with long-term response based on self-learning the system status and the efficiency of the security controls deployed.

AI4DECEIVE

The intelligent deception mechanisms that will enrich the response of the AI4SOAR.

AI4COLLAB

The service for automatic anonymous sharing of incident information.

Trustworthy AI

TRUST4AI

A set of highly innovative methods and models ensuring trustworthiness of AI systems.



Networking and cluster activities

AI4CYBER IS ACTIVELY EXPANDING ITS NETWORK BY ENGAGING WITH SISTER PROJECTS AND CLUSTERS.

- **The Cybersecurity Innovation Cluster for EPES, CyberEPES cluster**
<https://cyberseas.eu/cyberepes/>

The cluster acts as a think tank and information exchange ecosystem of EU-funded projects dealing with cybersecurity and resilience research and innovation on Electrical Power and Energy System (EPES) infrastructure.

- **The European Cluster for Securing Critical Infrastructures ECSCI cluster, coordinated by the EU-CIP project**
<https://www.finsec-project.eu/ecsci>

The cluster gathers together 31 EU-funded projects on the subject, 14 of which are still running. The banking use case in AI4CYBER will be the most relevant for this cluster. CXB is currently participating in some of the cluster projects.

- **The Cybersecurity Cluster in the Horizon Results Booster**
<https://www.horizonresultsbooster.eu/>

Initiative by the European Commission. Together with DYNAMO, KARTOS, ELECTRON and DYNABIC projects, AI4CYBER is participating in the "DYNAMO project group" led by DYNAMO project.

- **ENCRYPT project**

The collaboration included presenting AI4CYBER during the first clustering workshop organised by ENCRYPT with other EU projects (CROSSCON, CERTIFY, AI4CYBER, TRUSTEE, and KINAITICS).

- **The European Cybersecurity Competence Center (ECCC) EU Project Hub**
<https://radar.cyberwatching.eu/radar/>

- **The LAZARUS project**
Project (athenarc.gr)

- **The KINAITICS project**
Discover the whole KINAITICS project : missions, objectives...