AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

Project Summary

Erkuden Rios, Project Coordinator, tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Funded by the European Union

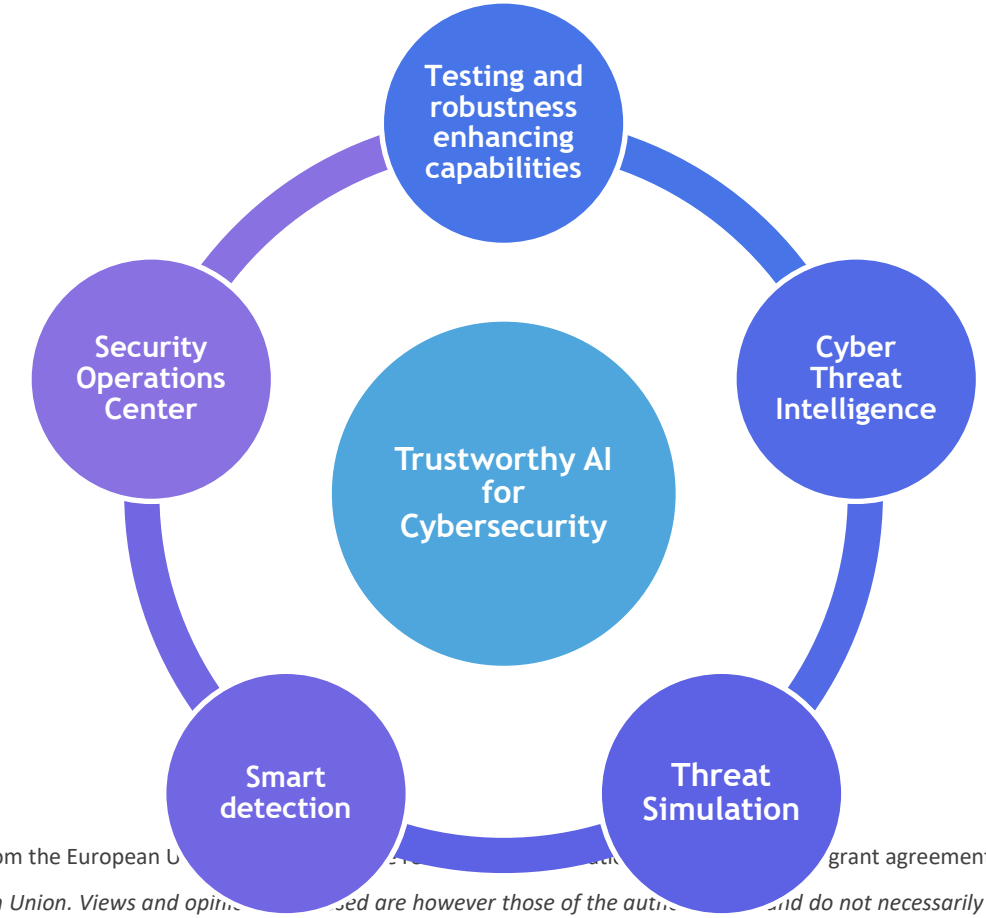
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER in a nutshell

Establishing an **Ecosystem Framework** of next generation **AI-based services** for critical system **robustness, resilience**, and appropriate **response in the face of advanced and AI-powered cyberattacks.**

11 Key Results that cover **6 cybersecurity areas**



3 Demonstrators that foster **innovation**

- **Energy**
- **Banking**
- **Health**

Funded by the European Union

This project has received funding from the European U grant agreement No 101070450.

AI4CYBER Ecosystem

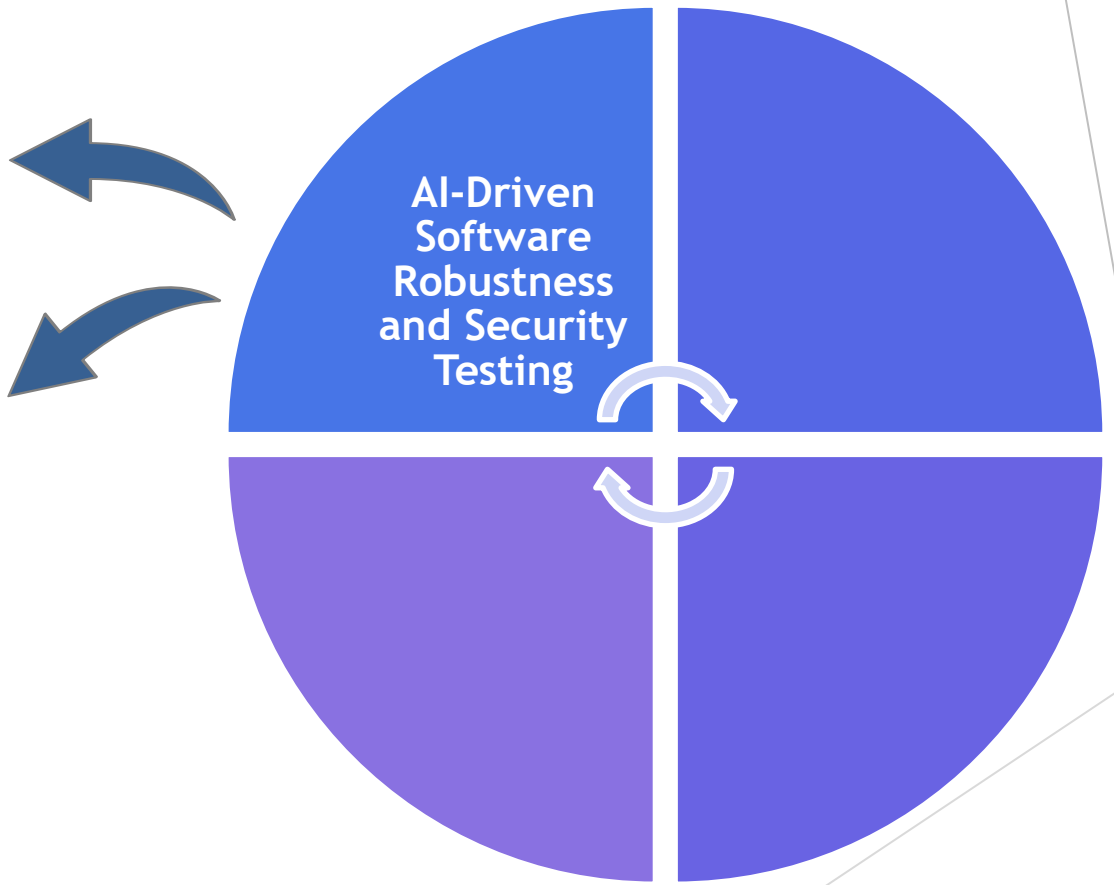
Tools & Services to be offered

AI4VULN - Code testing

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 - Vulnerability fixing

An 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



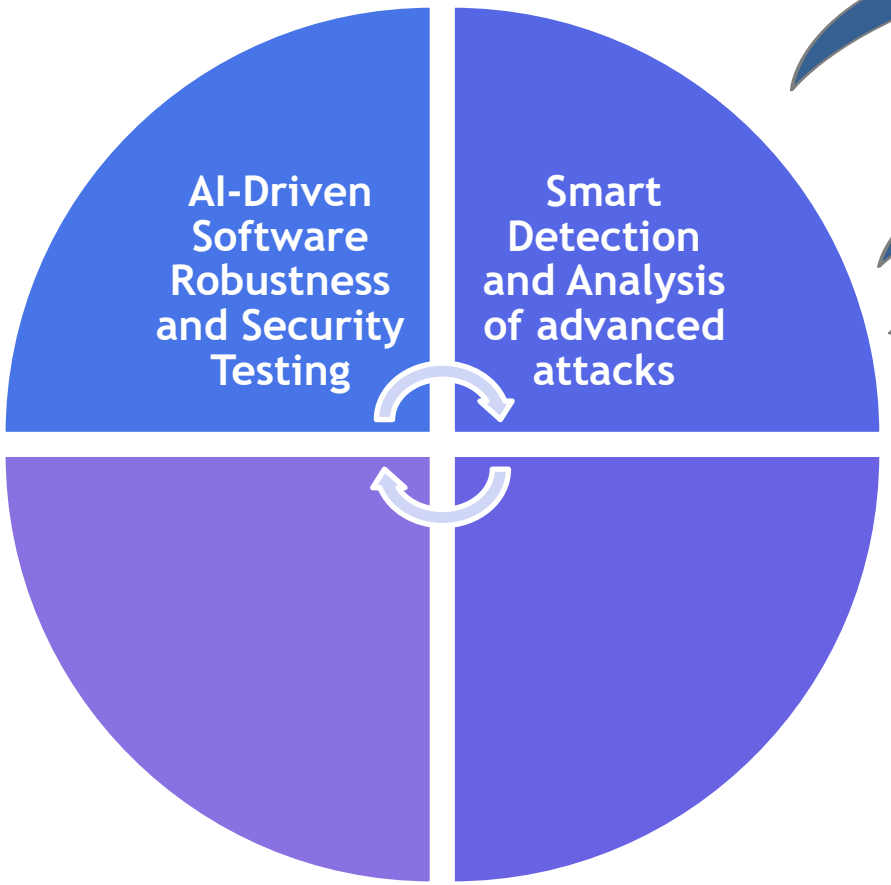
Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Ecosystem

Tools & Services to be offered



AI4FIDS - Federated Detection of threats

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

AI4TRIAGE - Incident triage

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

AI4SIM - Threat simulation

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

AI4CTI - Cyber Threat Intelligence improvement

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

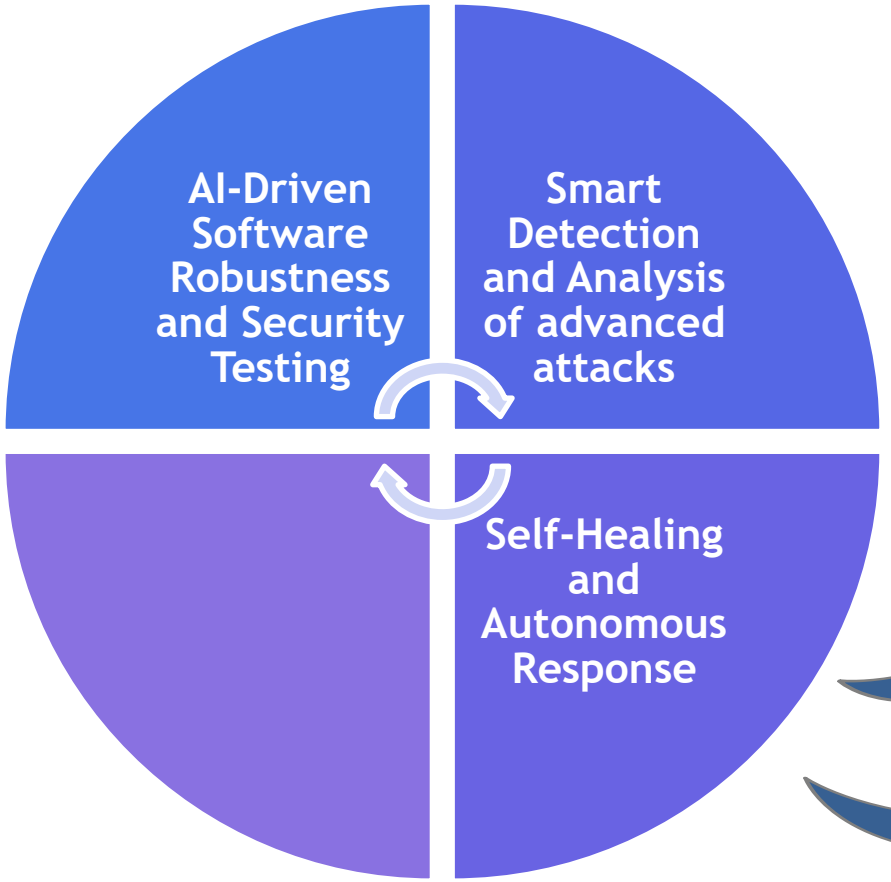
Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Ecosystem

Tools & Services to be offered



AI4SOAR - Security Orchestration, Automation and Response

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 - Long term adaptation

AI-based service that enriches the AI4SOAR with long-term response based on self-learning the system status and the efficiency of the security controls deployed

AI4DECEIVE - Deception and honeypots

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

AI4COLLAB -Information sharing and collaboration

Automatic anonymous sharing of incident information

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme unc

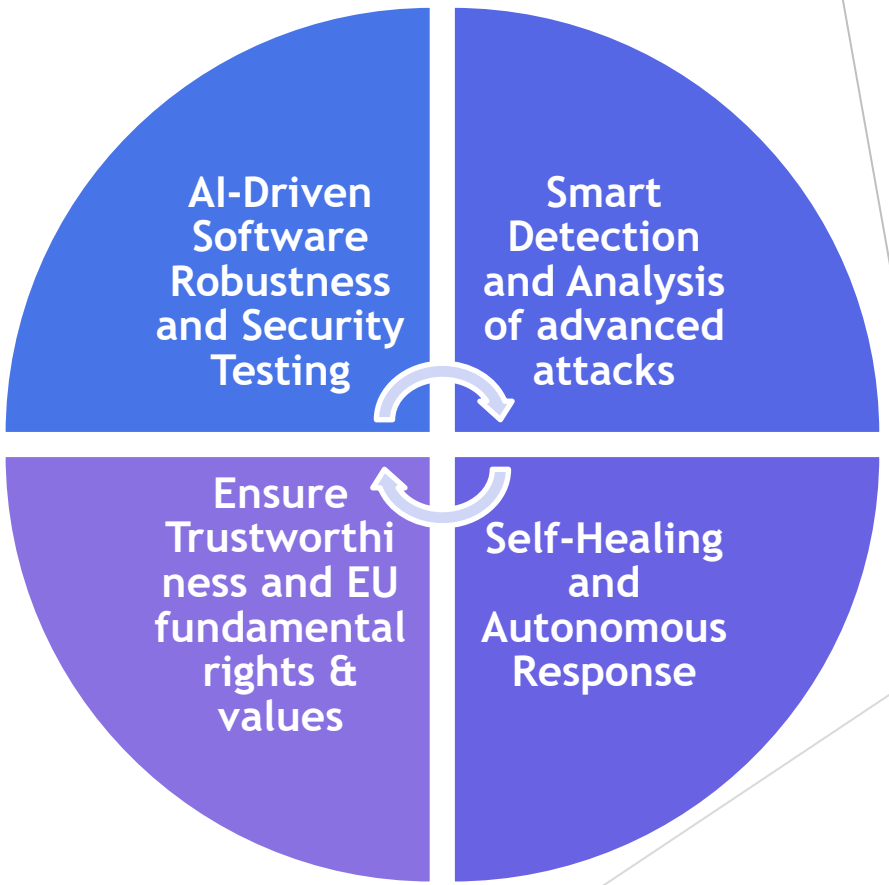
AI4CYBER

AI4CYBER Ecosystem

Tools & Services to be offered

TRUST4AI - Trustworthiness of AI

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



Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Impact and Added-Value

Ecosystem of AI-based cybersecurity reinforcement services

Enhanced **resilience** of critical products, systems and processes

Ensured secured disruptive technologies

Increased knowledge about AI-powered attacks to IT systems

Increased software and supply chain security

Reinforced awareness and common cyber security management and culture

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Use Cases ▸ Energy

Problems to solve

- Timely detection of AI-powered and advanced cyberattacks
- Timely prevention of AI-powered and advanced cyberattacks
- Gathering valuable information about malicious activities

Expected benefits

- Detection accuracy of energy-related cyberattacks ← Smart Detection related solutions (AI4FIDS, AI4TRIAGE, AI4SIM, AI4CTI)
- Optimized defence against energy-related cyberattacks ← SOAR related solutions (AI4SOAR, AI4ADAPT, AI4DECEIVE, AI4COLLAB)

Trustworthy AI

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Use Cases ▸ Banking

Problems to solve

- Fraud prevention and detection
- Internal fraud prevention and detection
- Information leakage and personal data protection

Smart Detection related solutions (AI4FIDS, AI4TRIAGE, AI4SIM, AI4CTI)

Expected benefits

- Reduced false positives and negatives in fraud detection
- Reduced vulnerabilities in source code
- Privacy-preserving detection of anomalies in user behaviour
- Optimized defence against AI-powered and advanced attacks

Testing related solutions (AI4VULN, AI4FIX)

SOAR related solutions (AI4SOAR, AI4ADAPT, AI4DECEIVE, AI4COLLAB)

Trustworthy AI

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER Use Cases ▸ Health

Problems to solve

- Vulnerability identification for security hardening of the systems
- Detection and response of AI-powered and advanced cyberattacks
- Sharing threat intelligence with multi-agent systems and privacy preservation

Expected benefits

- Simulation of AI-based and advanced cyberattacks to stress security controls
- Threat intelligence improving AI models for incident response and containment
- Detection accuracy of cyberattacks and able to identify zero-day attacks and modern offensive AI
- Autonomous response of processes to promptly react to incidents

Smart Detection related solutions (AI4FIDS, AI4TRIAGE, AI4SIM, AI4CTI)

SOAR related solutions (AI4SOAR, AI4ADAPT, AI4DECEIVE, AI4COLLAB)

Trustworthy AI

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER Timeline

Project implementation
September 2022 – August 2025

Stage 1 August 2023

Stage 2 August 2024

Stage 3 August 2025

Stage 1 - Design
Initial architecture of the AI4CYBER Framework

Stage 2 - First release
First release of the AI4CYBER Framework services and tools

Stage 3 - Final release
Final release of the AI4CYBER Framework services and tools

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

AI4CYBER project data

Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience

- **Coordinator:** **TECNALIA**
- **Consortium:** 13 partners; 7 EU MS
- **Project Type:** Research and Innovation
- **Grant Agreement ID:** 101070450
- **Start Date:** 1 September 2022
- **End Date:** 31 August 2025

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER consortium

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

MINDS

montimage

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

FRONTENDART

EOS
EUROPEAN ORGANISATION FOR SECURITY

PDM

iTTi

THALES

CaixaBank

ΔΕΗ

Hospital do Évora Espírito Santo E.P.E.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

https://ai4cyber.eu

https://twitter.com/Ai4Cyber

https://www.linkedin.com/company/ai4cyber/

Erkuden Rios

Project Coordinator

erkuden.ríos@tecnalia.com

Thank you for your attention!

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.