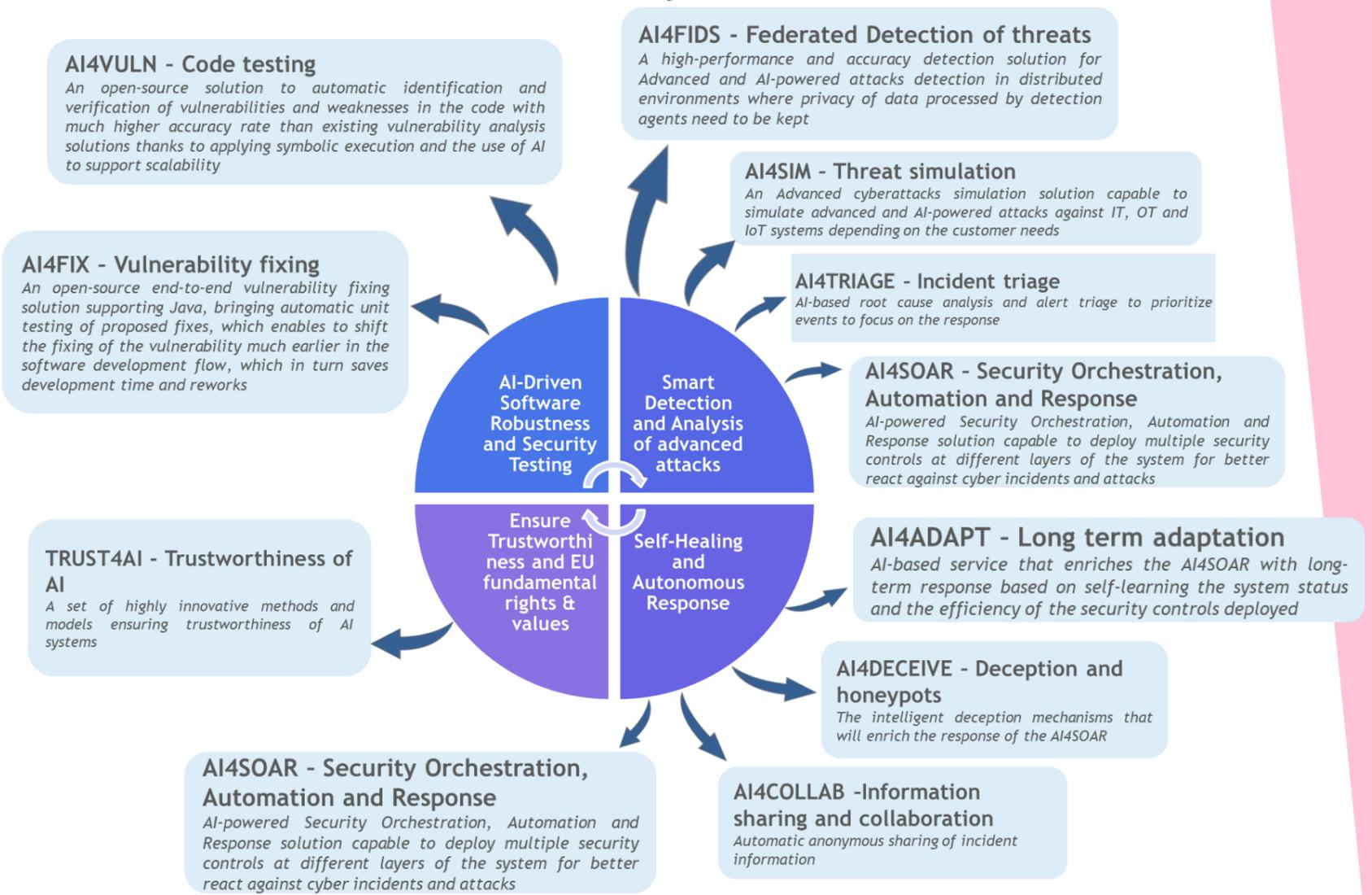# AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

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

AI4CYBER Ecosystem

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

TRUST4AI - Trustworthiness of AI
A set of highly innovative methods and models ensuring trustworthiness of AI systems

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

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

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

AI4TRIAGE - Incident triage
AI-based root cause analysis and alert triage to prioritize events to focus on the response

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

Central diagram segments:
- AI-Driven Software Robustness and Security Testing
- Smart Detection and Analysis of advanced attacks
- Ensure Trustworthiness and EU fundamental rights & values
- Self-Healing and Autonomous Response

The Team

tecnalia — MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

EOS — EUROPEAN ORGANISATION FOR SECURITY

iTTi

MINDS

THALES

SEARCH-LAB — SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

PDM

montimage

FRONTENDART

Sectors

CaixaBank — Banking

ΔΕΗ — Energy

Hospital do Espírito Santo E.P.E. — Health

Stay Updated

https://ai4cyber.eu/

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

https://twitter.com/Ai4Cyber