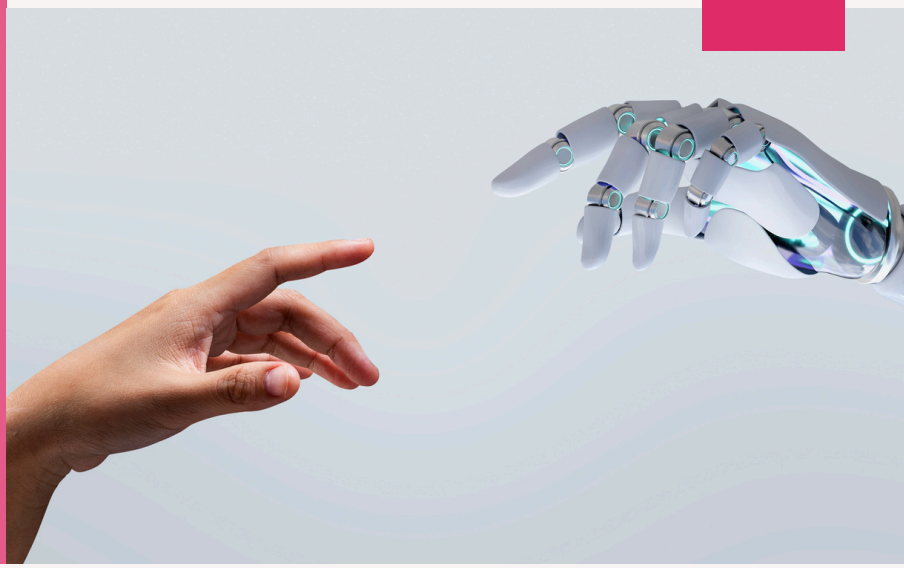
AI4CYBER

Solutions

Trustworthy AI for



01 TRUST4AI.Security

A mean to automate the search for all possible attack techniques and protections relevant to the AI under study. Therefore, it significantly facilitates the task of risks assessment in AI-based systems in regard to the risks to the AI robustness and security.

02 TRUST4AI.Fairness

A purpose to ensure that cybersecurity systems do not introduce bias and discrimination in the process on AI analyses

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. Disclaimer: Funded by the European Union. 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.

AI4CYBER

Solutions

AI for Response

01 AI4SOAR

An 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.

02 AI4ADAPT

An “intelligent” Reinforcement Learning (RL) solution with the main objective of optimizing the incident response adaptation. The component is designed to defend the victim system against certain types of attacks (advanced attacks in the AI4CYBER nomenclature) which are composed of a chain of different atomic 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. Disclaimer: Funded by the European Union. 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.

AI4CYBER

Solutions

AI for Response

03 AI4DECEIVE

Intelligent Deceive Decision Engine (IDDE) module applies game theory algorithms to determine the optimal type and number of honeypot instances needed to mitigate detected threats against a system under protection. The game theory-based models enable modelling attacker-defender interactions, planning deception strategies, and conducting cost-benefit analyses.

04 AI4COLLAB

Represents a transformative step forward in Cyber Threat Intelligence (CTI) sharing, seamlessly integrating MISP and OpenCTI platforms to enable a secure, real-time, and scalable exchange of threat data. Leveraging Apache Kafka for high-throughput processing, the platform ensures that CTI flows efficiently between stakeholders while complying with GDPR and preserving data utility.

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. Disclaimer: Funded by the European Union. 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.