AI4CYBER

Solutions

AI for Testing

01 AI4VULN

A static source code analyzer tool that can detect vulnerability problems in the source code. It uses symbolic execution, which means that it simulates the execution of the program without real execution and this way, it can detect runtime vulnerability issues in the code.

02 AI4FIX

Enables to shift the fixing of the vulnerability much earlier in the software development flow, which in turn saves development time and reworks. The tool can be used with online and offline large language models and it is able to generate tests to improve code coverage.

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 Detection

01 AI4CTI

An LLM-based Cyber Threat Intelligence knowledge analyzer and aggregator, which primary goal is to gather insights from public cyber threat intelligence (CTI) platforms and to identify the techniques and attack paths commonly used by threat actors in sophisticated cyber-attacks.

02 AI4FIDS

A high-performance solution designed to detect a broad spectrum of attacks across network, host, and log data. Its core feature is federated learning, allowing multiple clients to collaboratively train an intrusion detection model without sharing their raw data.

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 Detection

03 AI4SIM

LLM-based attack technique generator is a python prototype that allows the automatic creation and execution of diverse attack technique codes. The generated TTP code adheres to the TTPs defined in the MITRE ATT&CK Enterprise framework, which is the world-wide de-facto standard for TTPs taxonomy

04 AI4TRIAGE

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

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.