AI4CTI

LLM-based CTI aggregator

LLM-based Cyber Threat Intelligence knowledge analyzer and aggregator, whose 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.The module retrieves CTI data from carefully selected open sources on the internet, the widely used CISA advisories and the attack reports by AttackIQ company.

AI4CYBER Component

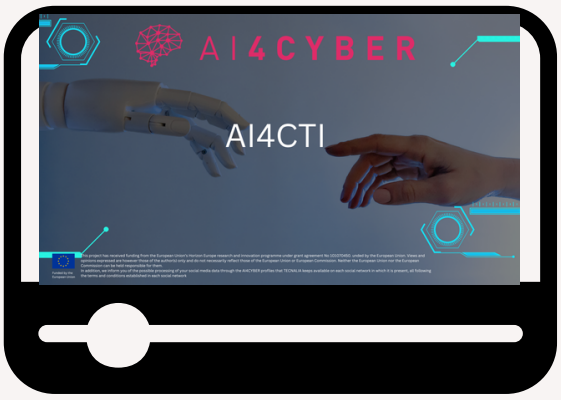
The solution supports security engineering efforts by helping analyze large volumes of threat-related information. Most importantly, the solution aids in the identification and understanding of the attack technique sequences of the attacks as well as the most appropriate mitigation to counter the attack steps and stop the attack or minimize the impact.

AI4CTI is a LLM-powered analyser and aggregator of CTI information. In particular, in the AI4CYBER context, the work focused on threats relevant to the AI4CYBER use cases.

The CTI source types analysed by AI4CTI are:

- Structured data from security advisories, in particular from both CISA advisories, which are authoritative reports produced by cybersecurity experts from the U.S. Department of Homeland Security, and advisories-related reports from AttackIQ.
- Unstructured natural language descriptions in advisories that describe the attack scenarios.
- Attack flow information in graph representations.

The output of AI4CTI consists of a curated set of tactics, techniques, and procedures (TTPs), along with corresponding mitigation strategies extracted from the source data. Through a process of cross-referencing and validating information across multiple sources, the module determines the chronological sequence of TTPs used in attacks and maps the appropriate mitigations to each step. The LLM leveraged by the component is the Reduced Llama-3.1-70B-Instruct which demonstrated consistently strong performance.



YouTube Video Link

The solution is still a prototype and the future tool will have commercial license.

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Erkuden Rios (Erkuden.rios@tecnalia.com)
Fundación Tecnalia Research & Innovation.

www.tecnalia.com
https://es.linkedin.com/company/tecnalia-research-innovation
https://x.com/tecnalia

E. Iturbe, E. Rios, A. Rego, and N. Toledo, "Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework", in Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–8.

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.