AI4COLLAB

AI-based Threat Information Sharing Platform

Designed to facilitate the sharing of CTI with CTI communities, leveraging AI along with the MISP and OpenCTI platforms. While employing both MISP and OpenCTI platforms to extend the reach to CTI communities, AI4COLLAB leverages AI to automatically detect and redact sensitive or private information in the CTI data to be shared.

AI4CYBER

Ccomponent

The AI4COLLAB solution provides:

- Automatic AI-powered anonymisation: AI4COLLAB employs multiple techniques, including LLMs and Microsoft Presidio, to detect and automatically anonymise sensitive content of CTI data. This functionality minimises human mistakes.
- Standardised and flexible integration: AI4COLLAB can integrate with external STIX-compatible CTI sources using Apache Kafka.
- Broad CTI support: AI4COLLAB combines both MISP and OpenCTI platforms and allowing the ingress CTI information to be anonymised and shared seamlessly to both MISP and OpenCTI, thus extending the reach to CTI communities.

AI4COLLAB is an AI-powered platform for sharing Cyber Threat Intelligence (CTI), 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.

A standout feature of AI4COLLAB is its advanced anonymization pipeline, which combines Microsoft Presidio with Large Language Models (LLMs) to automatically detect and redact sensitive information with approximately high accuracy. This robust anonymization capability significantly reduces privacy risks without compromising the value of shared intelligence. By supporting open standards such as MISP, Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) and adopting the Server-Sent Events (SSE) protocol for real-time updates, AI4COLLAB ensures broad interoperability and seamless integration with existing cybersecurity infrastructures. Designed for cybersecurity providers, enterprise SOCs, and governmental bodies, AI4COLLAB not only strengthens collaborative defense mechanisms but also unlocks pathways for commercialization through IP protection. The component's innovation and impact make it a cornerstone for future-ready, AI-powered CTI ecosystems.

YouTube Video Link

The solution is provided in dual license. The open-source version includes both CTI platforms and utilises Microsoft Presidio as the anonymisation method. The commercial version is closed source and supports anonymisation using LLMs. https://gitlab.ithaca.ece.uowm.gr/ai4cyber/ai4collab

UNIVERSITY OF WESTERN MACEDONIA

Panagiotis Radoglou-Grammatikis (pradoglou@uowm.gr)
University of Western Macedonia (UOWM)

https://www.uowm.gr/

C. Dalamagkas, D. Asimopoulos, P. Radoglou-Grammatikis et al., “AI4COLLAB: An AI-based Threat Information Sharing Platform,” 2024 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, pp. 783–788, Sept. 02, 2024. doi: 10.1109/csr61664.2024.10679429.

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.