AI4SIM

MAIP, the Montimage AI Platform

MAIP is part of AI4SIM and TRUST4AI. Security for the generation of adversarial attacks . It offers a user-friendly interface and APIs for interacting with various AI services, including feature extraction, model building or retraining, adversarial attack injection, model explanation, and evaluation using different datasets. The platform aims to enhance the resilience and security of network systems through explainable AI techniques.

AI4CYBER

Ccomponent

AI4SIM provdes:

·Adversarial Robustness: Includes features for injecting adversarial attacks to evaluate and improve model robustness.

·Enhanced Security: Utilizes AI to detect anomalies and potential threats in network traffic, improving overall security posture.

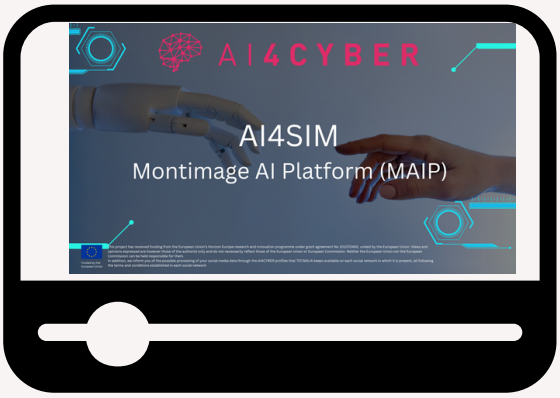
·Explainable AI: Incorporates LIME and SHAP for model interpretability, aiding in understanding and trust of AI decisions.

·Modular Architecture: Supports various AI services, allowing customization and extension to meet specific needs.

·Integration Ready: Provides APIs for seamless integration with existing systems and workflows.

MAIP (Montimage AI-powered Platform) is a modular framework that centralizes Montimage's AI services for network traffic analysis, anomaly detection, and cybersecurity evaluation.

Beyond traditional AI capabilities, MAIP provides advanced functionality for adversarial testing, including the generation and injection of adversarial traffic to evaluate the robustness of machine learning models. For example, it leverages Generative Adversarial Networks (GANs) to simulate realistic data poisoning attacks, where malicious inputs are crafted to compromise model accuracy or evade detection. By incorporating these adversarial techniques, MAIP allows security teams to stress-test AI models under realistic threat conditions, ensuring that deployed solutions remain effective even against sophisticated evasion strategies. It also integrates explainable AI tools, such as LIME and SHAP, to help analysts understand both normal and adversarial predictions, providing transparency in model behavior even in the presence of attacks. With its combination of adversarial robustness testing, explainable AI, and real-time analytics, MAIP empowers organizations to proactively identify vulnerabilities in AI-based security systems and improve their resilience against emerging cyber threats.



YouTube Video Link

The solution is still a prototype and the future tool will have commercial license. The MAIP is hosted as an open-source project in Montimage GitHub repository under the Apache-2.0 licence. https://github.com/montimage-projects/maip

Manh Dung Nguyen (manhdung.nguyen@montimage.eu)
Montimage

https://www.montimage.eu/

EManh-Dung Nguyen, Anis Bouaziz, Valeria Valdes, Ana Rosa Cavalli, Wissam Mallouli, Edgardo Montes de Oca. A deep learning anomaly detection framework with explainability and robustness. In the 18th International Conference on Availability, Reliability and Security (ARES 2023) pp 134:1-134:7. Benevento, Italy. August 29, 2023. https://dl.acm.org/doi/10.1145/3600160.3605052

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.