SENTAI

End users

Republic of North Macedonia
Ministry of digital transformation

MARnet
MACEDONIAN ACADEMIC
RESEARCH NETWORK

AMRES
Akademska mreža Srbije

Partners

"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

The Faculty of Computer Science and Engineering (FINKI) within UKIM, is the largest and most prestigious faculty in the field of computer science and technologies in North Macedonia. FINKI has a strong research background in a diverse set of research topics founded in the fields of complex networks, data science, arti-ficial intelligence and high-performance com-puting.

University of Niš
Faculty of Electronic Engineering

The Faculty of Electronic Engineering (FEL) at the University of Niš in Serbia is a leading institution in the fields of electrical engineer-ing, computer science, telecommunications, and electronics. It is renowned for its com-prehensive academic programs and cutting-edge research in areas such as artificial intelligence, machine learning, power engi-neering, and microelectronics.

Sentinel AI: Enhancing Cybersecurity Through Artificial Intelligence

NATO Science for Peace and Security Multi Year Project

Get in touch

https://sentai-project.io/

SENTAI@finki.ukim.mk

https://www.linkedin.com/company/sentai-project

SENTAI

Context

Network security continues to face escalating threats, with cyber-attacks increasingly targeting critical infrastructure and causing billions in global damages. Despite decades of research, traditional security measures remain inadequate against these fast-evolving threats.

Current AI-based intrusion detection systems offer some improvements but are limited by outdated training models, siloed system design, inadequate real-world validation, and challenges in handling large-scale data. These weaknesses reduce their effectiveness in modern, high-speed threat environments.

The SENTAI project addresses these gaps by proposing a unified, AI-driven cybersecurity platform. It integrates diverse data sources, employs up-to-date training techniques, and utilizes cloud-based processing for scalable, real-time threat detection. SENTAI's adaptive, comprehensive approach aims to deliver more accurate, efficient, and resilient protection against today's complex cyber threats.

With continuous learning and scalable architecture, SENTAI enables faster response and stronger defense against evolving cyber risks.

Objectives

Goal

The goal of the SENTAI project is to develop an AI-based cybersecurity system that integrates diverse, up-to-date datasets for accurate threat detection, ensures real-world applicability through realistic scenario testing, and addresses big data challenges with robust infrastructure for efficient analysis and timely threat response.

Mission

- Enhance cybersecurity through an AI-driven, end-to-end solution
- Automate data collection and transformation for efficient processing
- Apply artificial intelligence for advanced threat detection and analysis
- Deliver clear threat presentation and intuitive visualisation for rapid response

Impact

The project aims to significantly improve cybersecurity by integrating diverse datasets and developing comprehensive AI-based solutions. This will enhance the effectiveness of cybersecurity measures, including reduced response time, increased detection rates, and minimized false positives.

Key outcomes

- Develop an AI cybersecurity system for real-world use
- Use diverse data for training and testing
- Test against realistic scenarios
- Build infrastructure for big data analysis
- Provide outputs that are FAIR, open, and intended for broad adoption.
- Enable end users to practically deploy the developed solutions enabling them better network security
- Provide training and support for young researchers