Republic of North Macedonia
Ministry of Education and Science

European Commission
Joint Research Center (JRC)
of the European Commission

FACULTY OF MECHANICAL ENGINEERING

SENTAI
Sentinel AI: Enhancing Cybersecurity Through Artificial Intelligence

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

University of Niš
Faculty of Electronic Engineering

1. CONTEXT

Network security continues to face escalating threats, with cyberattacks 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 Current AI-based intrusion detection systems offer some improvements but are limited by outdated training models, siloed system design, inadequate real-world validation, and challenges in handling large-scale data.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 developing a unified, AI-driven cybersecurity platform.

2. OBJECTIVES

GOALS

- Develop an AI-based cybersecurity system
- Integrate diverse, up-to-date datasets for accurate threat detection
- Ensure real-world applicability through realistic scenario testing
- Address big data challenges with robust infrastructure
- Enable 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 visualization for rapid response

3. DESIGN

SENTAI 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.

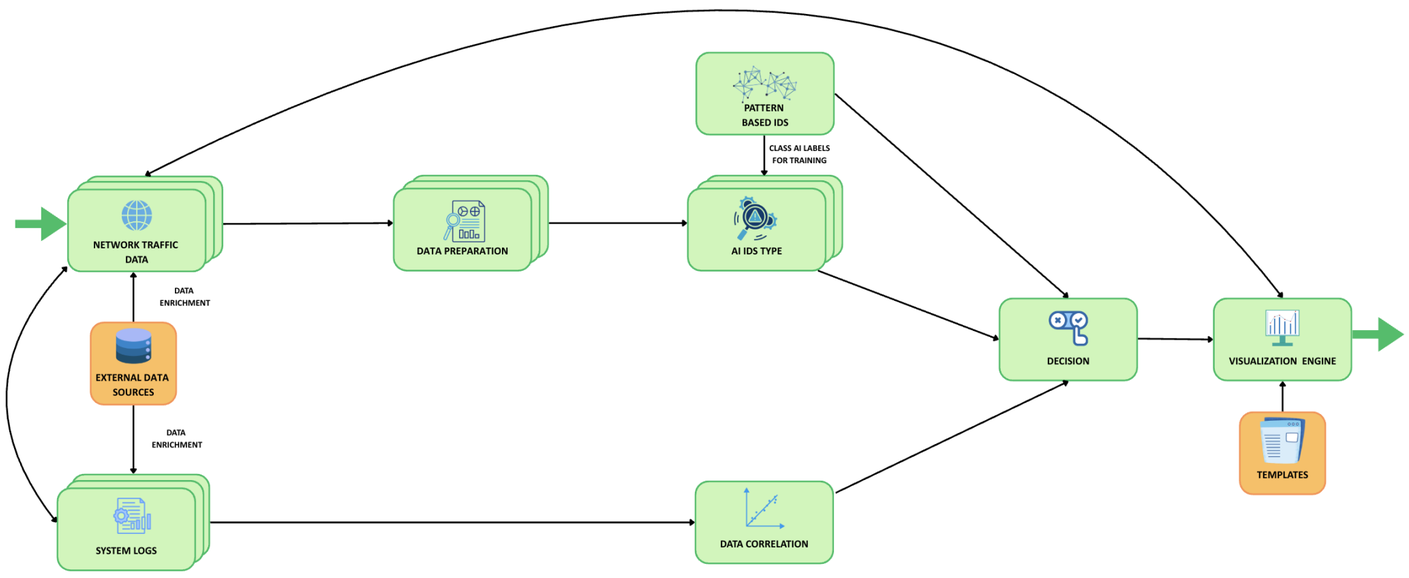

Figure 1. The conceptual model of the proposed security system

4. KEY OUTCOMES

Train and Test with Diverse Data
Use varied and up-to-date datasets to reflect real-world conditions and improve model robustness.

Test Against Realistic Scenarios
Evaluate AI models under practical conditions, including different attacks and system behaviours.

Build Infrastructure for Big Data Analysis
Design scalable systems to process and analyse large volumes of cybersecurity data efficiently.

Ensure FAIR and Open Outputs
Deliver results and tools that are easily Findable, Accessible, Interoperable, and Reusable.

Support Practical Deployment for End Users
Enable stakeholders to apply developed tools effectively, improving security in their environments.

Train and Mentor Young Researchers
Provide mentoring and hands-on experience for early-career professionals in AI cybersecurity.

5. IMPACT

This project drives major improvements in cybersecurity by developing AI-based solutions grounded in diverse, real-world data. By integrating advanced analytics and scalable infrastructure, it enhances threat detection accuracy, reduces response times, and minimises false positives.

The outcomes designed for practical deployment ensure that end users, including public and private sector organisations, can confidently adopt these tools to improve their digital security posture.

Contact
sentai-project.io
SENTAI@finki.ukim.mk
linkedin.com/company/sentai-project

SENTAI

NATO OTAN
This project is supported by: The NATO Science for Peace and Security Programme