Programme Slovakia

Newsletter
1/2026

Research and development of advanced artificial intelligence solutions for the detection of cyber threats and defense against sophisticated attacks

cybersecurityresearch-en.sk

Co-funded by the European Union

PROGRAMME SLOVAKIA

MINISTRY OF EDUCATION, RESEARCH, DEVELOPMENT AND YOUTH OF THE SLOVAK REPUBLIC

Project: Research and development of advanced artificial intelligence solutions for the detection of cyber threats and defense against sophisticated attacks

The project Research and Development of Advanced Artificial Intelligence Solutions for the Detection of Cyber Threats and Defense against Sophisticated Attacks addresses the increasing sophistication of cyber threats, for which traditional signature-based security solutions are becoming insufficient. Attackers are increasingly employing a combination of automated techniques, artificial intelligence, and behavioral manipulation, necessitating a shift from reactive approaches toward predictive and adaptive detection models.

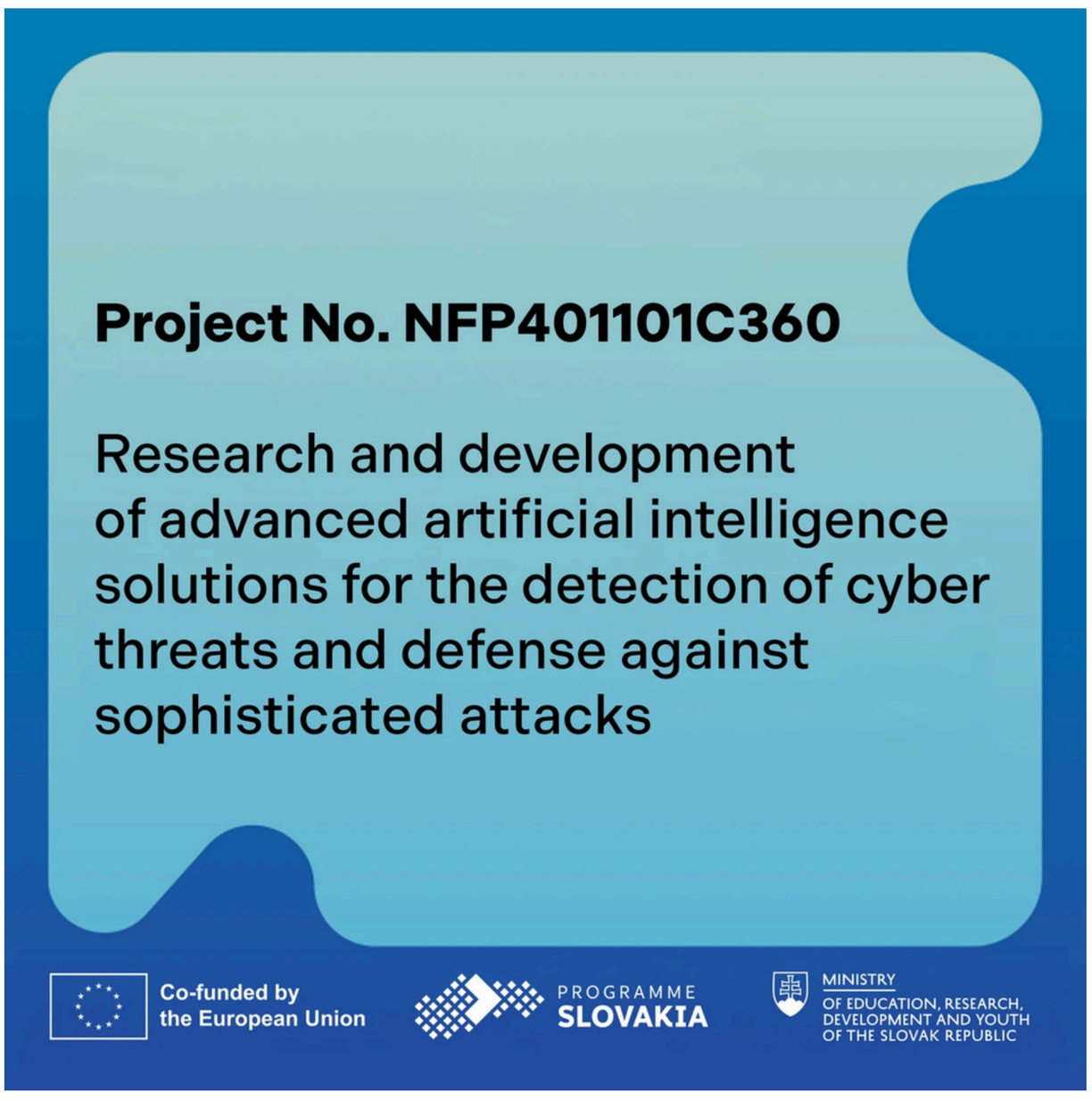
The main objective of the project is to investigate methods, approaches, and tools for the effective detection of advanced cyberattacks employing specific adversarial tactics, such as exploitation, lateral movement, and privilege escalation, in accordance with the MITRE ATT&CK framework. Particular emphasis is placed on the analysis of techniques, sub-techniques, and procedures (TTPs), the identification of their distinguishing characteristics, and the discovery of limitations in existing detection approaches.

The project also focuses on the behavioral analysis of attacks, the identification of Indicators of Compromise (IoCs) and Indicators of Behavior (IoBs), as well as the design of advanced models utilizing machine learning and artificial intelligence for anomaly detection across different stages of cyberattacks. The proposed solution includes the optimization of detection accuracy and efficiency, together with validation under realistic conditions through the simulation of cyberattacks.

The project contributes to strengthening the resilience of digital infrastructure, supporting the development of domestic research capacities, facilitating knowledge transfer between academia and industry, and enhancing Slovakia's cyber resilience within the broader European context.

The main project outputs include a research report on cyberattack tactics and techniques, a simulation platform for threat analysis and detection, advanced machine learning and statistical lear

Co-financed by the European Union through the Slovakia Programme under project No. NFP401101C360: Research and development of advanced artificial intelligence solutions for the detection of cyber threats and defense against sophisticated attacks.



Co-funded by the European Union
PROGRAMME SLOVAKIA
MINISTRY OF EDUCATION, RESEARCH, DEVELOPMENT AND YOUTH OF THE SLOVAK REPUBLIC

The project develops advanced AI solutions for cyber threat detection

The research activities of project NFP401101C360: Research and Development of Advanced Artificial Intelligence Solutions for the Detection of Cyber Threats and Defense against Sophisticated Attacks, introduce novel approaches to the detection of sophisticated cyber threats through the application of machine learning and behavioral analysis of cyberattacks.

The project focuses on the development of methods and tools enabling the reliable detection of advanced cyberattacks, particularly those involving exploitation, lateral movement, and privilege escalation in accordance with the MITRE ATT&CK framework. The research also investigates the limitations of current detection approaches and explores opportunities to improve their accuracy under real-world conditions.

An important component of the project is the comprehensive analysis of techniques, sub-techniques, and procedures (TTPs). This includes identifying their characteristic manifestations and examining the tools employed in the execution of cyberattacks. The project also encompasses the simulation of cyber incidents in a secure testing environment and the validation of various detection scenarios.

Another research area is the behavioral analysis of cyberattacks based on forensic and network data. The objective is to identify Indicators of Compromise (IoCs) and Indicators of Behavior (IoBs), as well as to determine operating system and network communication parameters that can contribute to more effective cyber threat detection.

A significant aspect of the project is the design of new models based on machine learning, artificial intelligence, and mathematical modelling. These models are intended for anomaly and attack detection across multiple stages of system compromise. Particular attention is devoted to optimizing the performance of detection models with an emphasis on accuracy, sensitivity, and reduced computational requirements.

The project also contributes to the development of professional capacities in the field of cybersecurity. The research results will be gradually integrated into university courses focused on cybersecurity and information security, as well as data analytics.

Project researchers participated in a conference on crisis management

The project researchers, prof. Milan Kubina and prof. Segeč, participated in the conference "*Resolving Crisis Situations in a Specific Environment*", which was held under the auspices of the University of Zilina in Zilina and the Ministry of the Interior of the Slovak Republic.

From the perspective of the project, they were most interested in the panel discussion on the topic "I", which included stimulating opinions on the current challenges and direction of cybersecurity.

Co-funded by the European Union
PROGRAMME SLOVAKIA
MINISTRY OF EDUCATION, RESEARCH, DEVELOPMENT AND YOUTH OF THE SLOVAK REPUBLIC