



Newsletter 2/2026

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

Workshop on protection against ransomware attacks

In July, a workshop focused on the ransomware protection toolkit GRYPHON by IstroSec was held at the Faculty of Management and Informatics, UNIŽA. Participants learned about the tool's functionality and its potential use in protection against ransomware attacks. The workshop, led by lecturer Kristína Glončáková, included an expert presentation as well as space for discussion, during which participants' questions were answered.

Bridging academic research and industry practice: a new research workplace

Strong projects are not built in laboratories alone. They emerge where research meets practice. One of the key contributions of the project is therefore the connection of the academic environment with technological practice in the field of cybersecurity.

The establishment of a joint research workplace between UNIŽA, TUKE, ICE and the companies IstroSec and Syteli is creating an interdisciplinary team that combines practical experience with the analytical capacities of universities. This collaboration provides an opportunity for researchers to develop their professional skills and to gain new knowledge in the field of artificial intelligence and cybersecurity.

Researchers will take part in specialised training sessions and workshops organised in cooperation with IstroSec, focused on advanced analysis of cyber threats and the detection of attacks using artificial intelligence.

The collaboration also includes practical testing scenarios, with participants working on real security incidents as well as simulated cyberattacks, which will help them better understand how security incidents are resolved in practice and develop skills relevant to their future professional work.

The project also supports the development of professional contacts and long-term partnerships that can be used in future projects related to security operations centers.

The project will also involve testing and validating neural networks and autoencoders, as well as exploring graph-based models that can help identify exploitation, lateral movement and privilege escalation.

The research results will be published in scientific journals and presented at conferences, contributing to the wider dissemination of knowledge in cybersecurity at an international level.



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

Towards intelligent security operations centers

Traditional security approaches are increasingly unable to keep pace with how quickly cyber threats evolve. The project therefore also focuses on the shift from traditional security operations towards a new generation of intelligent security operations centres, capable of automating the analysis of security incidents to detect attacks faster and make more efficient use of security teams' capacities.

The solution also includes adaptive detection mechanisms that can learn from new attacks and identify threats even without the use of malware signatures.

The project's outputs will be applicable particularly in areas where cyber resilience is critically important, such as critical infrastructure, banking, telecommunications and industrial manufacturing.

The project's own AI based security solutions can also help reduce dependence on foreign technologies. The new detection models will be compatible with existing security systems, enabling their faster adoption in real world operation without the need for extensive changes to infrastructure.

Can machine learning detect malware more accurately than humans? And where are its limits?

These were among the key questions explored during a workshop at Machine Learning Summer School @UNIZA 2026, held from 14 to 18 September at the Faculty of Management Science and Informatics of the University of Žilina.

As part of the project Research and development of advanced artificial intelligence solutions for the detection of cyber threats and defense against sophisticated attacks, IstroSec contributed to the programme with a workshop connecting two areas closely related to its expertise: cybersecurity and artificial intelligence. The workshop was led by Peter Písařík, R&D Specialist at IstroSec.

The workshop covered:

- how malware works and why its detection is becoming increasingly challenging,
- tools that help analysts identify threats more accurately,
- testing models with different architectures on specially prepared, harmless binary samples,
- reverse engineering supported by LLMs and how it is changing the work of analysts in practice.

The workshop was accompanied by an open discussion and a large number of questions from the participants. Their active engagement highlighted the broad potential for discussion around the intersection of cybersecurity, machine learning and artificial intelligence.

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.

