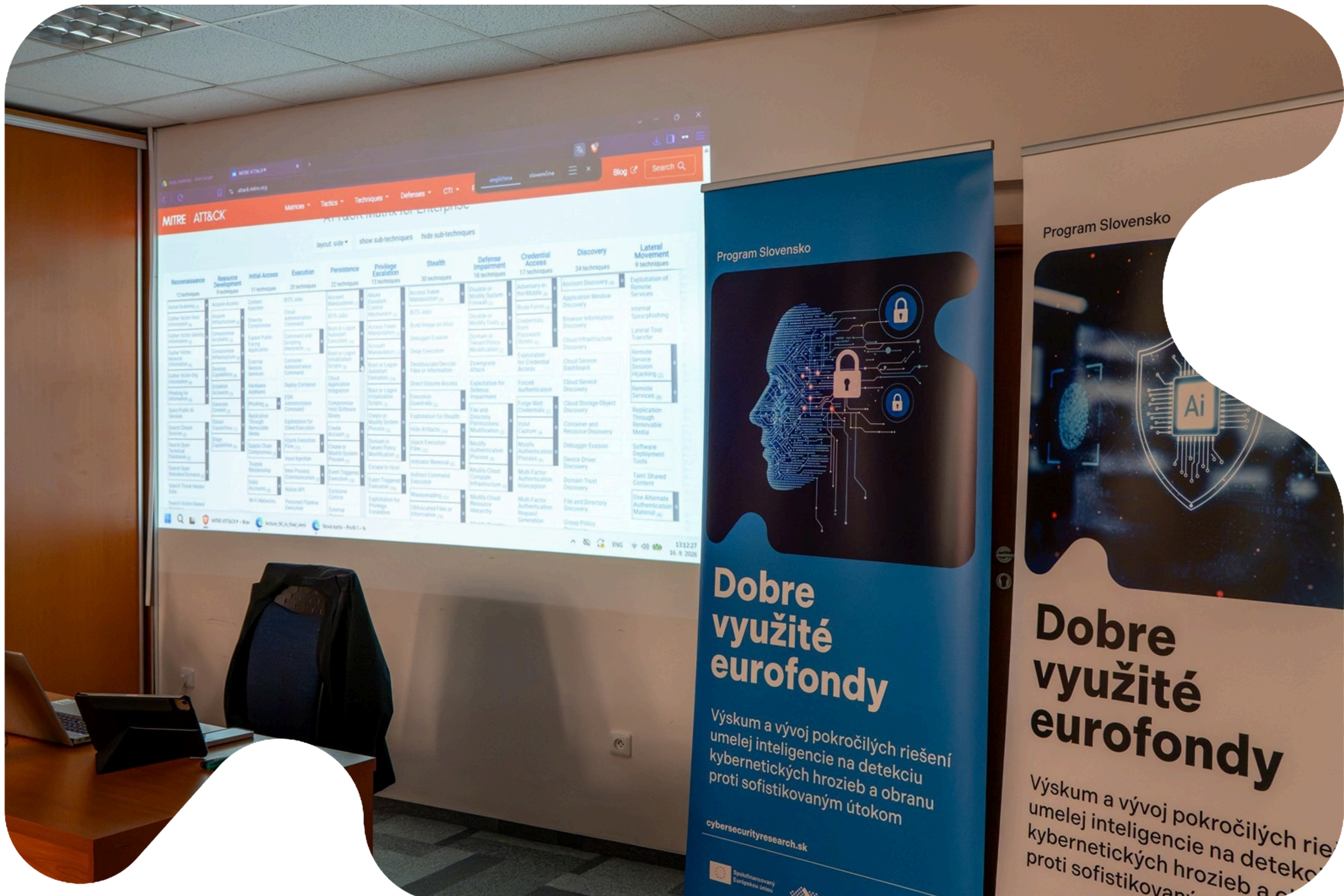




Newsletter

2/2026

Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom

cybersecurityresearch.sk



Spolufinancovaný
Európskou úniou



PROGRAM
SLOVENSKO



MINISTERSTVO
ŠKOLSTVA, VÝSKUMU,
VÝVOJA A MLÁDEŽE
SLOVENSKEJ REPUBLIKY

Workshop o ochrane pred ransomvérovými útokmi

Dňa 24. júla 2026 sa na Fakulte riadenia a informatiky Žilinskej univerzity uskutočnil workshop zameraný na ransomware protection toolkit GRYPHON od spoločnosti IstroSec. Účastníci sa oboznámili s fungovaním nástroja a možnosťami jeho využitia pri ochrane pred ransomvérovými útokmi.

Workshop pod vedením lektorky Kristíny Glončákovej zahŕňal odborný výklad a priestor na diskusiu, počas ktorej boli zodpovedané otázky účastníkov.

Spolupráca akademickej praxe a technológie: nové výskumné pracovisko

Silné projekty nevznikajú len v laboratóriách, ale najmä tam, kde sa stretáva výskum s praxou. Jedným z dôležitých prínosov projektu je preto prepájanie akademickeho prostredia s technologickou praxou v oblasti kybernetickej bezpečnosti.

Vznikom spoločného výskumného pracoviska medzi UNIZA, TUKE, ICE a spoločnosťami IstroSec a Syteli vzniká interdisciplinárny tím, ktorý prepája skúsenosti z praxe s analytickými kapacitami univerzít. Táto spolupráca vytvára priestor na rozvoj odborných kompetencií výskumníkov a podporuje získavanie nových znalostí v oblasti umelej inteligencie a kybernetickej bezpečnosti.

Výskumníci sa zapoja do špecializovaných školení a workshopov v spolupráci so spoločnosťou IstroSec, zameraných na pokročilú analýzu kybernetických hrozieb a detekciu útokov s využitím umelej inteligencie.

Súčasťou spolupráce sú aj testovacie scenáre. Účastníci budú pracovať s reálnymi bezpečnostnými incidentmi aj so simulovanými kybernetickými útokmi, čo im pomôže lepšie pochopiť riešenie bezpečnostných incidentov v praxi a rozvíjať zručnosti využiteľné v ich ďalšom odbornom pôsobení. Projekt zároveň podporuje rozvoj profesijných kontaktov a dlhodobých partnerstiev, ktoré môžu byť využité pri ďalších projektoch v oblasti bezpečnostných operačných centier.

V rámci projektu bude prebiehať testovanie a validácia neurónových sietí a autoenkodérov, ako aj skúmanie grafových modelov, ktoré môžu pomôcť pri identifikácii exploatacie, laterálneho pohybu a eskalácie privilégií.

Výsledky výskumu budú publikované vo vedeckých časopisoch a prezentované na konferenciách, čím prispejú k rozšíreniu poznatkov v oblasti kybernetickej bezpečnosti aj na medzinárodnej úrovni.

Dobre využité eurofondy

Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom



Spolufinancovaný
Európskou úniou



PROGRAM
SLOVENSKO



MINISTERSTVO
ŠKOLSTVA, VÝSKUMU,
VÝVOJA A MLÁDEŽE
SLOVENSKEJ REPUBLIKY



Spolufinancovaný
Európskou úniou



PROGRAM
SLOVENSKO



MINISTERSTVO
ŠKOLSTVA, VÝSKUMU,
VÝVOJA A MLÁDEŽE
SLOVENSKEJ REPUBLIKY

Smerom k inteligentným bezpečnostným operačným centrám

Tradičné bezpečnostné prístupy už často nestačia na tempo, akým sa menia kybernetické hrozby. Projekt sa preto zameriava aj na posun od tradičných bezpečnostných operácií k inteligentným bezpečnostným operačným centrám novej generácie, ktoré dokážu automatizovať analýzu bezpečnostných incidentov a tým rýchlejšie odhaľovať útoky a efektívnejšie využívať kapacity bezpečnostných tímov.

Súčasťou riešenia sú aj adaptívne detekčné mechanizmy, ktoré sa dokážu učiť z nových útokov a identifikovať hrozby aj bez použitia signatúr malvéru.

Výstupy projektu budú využiteľné najmä v oblastiach, kde je kybernetická odolnosť mimoriadne dôležitá, ako sú kritická infraštruktúra, bankovníctvo, telekomunikácie a priemyselná výroba.

Vlastné bezpečnostné riešenia využívajúce umelú inteligenciu môžu zároveň pomôcť znížiť závislosť od zahraničných technológií. Nové detekčné modely budú kompatibilné s existujúcimi bezpečnostnými systémami, čo umožní ich rýchlejšiu adopciu v reálnej prevádzke bez potreby rozsiahlych zmien infraštruktúry.

Dokáže strojové učenie odhaliť malvér presnejšie ako človek? A kde sú jeho limity?

Práve týmito otázkami sa venoval workshop na Machine Learning Summer School @UNIZA 2026, ktorá sa konala 14. až 18. septembra na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline.

V rámci projektu Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom sa spoločnosť IstroSec podieľala na programe workshopom, ktorý spojil dve oblasti úzko prepojené s jej odborným zameraním: kybernetickú bezpečnosť a umelú inteligenciu. Workshop viedol Peter Pisarcík, R&D Specialist, IstroSec.

Témami workshopu boli:

- ako funguje škodlivý softvér a prečo je jeho detekcia čoraz náročnejšia,
- nástroje, ktoré pomáhajú analytikovi presnejšie identifikovať hrozby,
- testovanie modelov rôznych architektúr na špeciálne pripravených, neškodných binárnych vzorkách,
- reverzné inžinierstvo s podporou LLM a spôsob, akým mení prácu analytika v praxi.

Workshop sprevádzala otvorená diskusia a množstvo otázok zo strany účastníkov. Aktívne zapojenie účastníkov ukázalo, že témy na rozhraní kybernetickej bezpečnosti, strojového učenia a umelej inteligencie ponúkajú priestor na širokú odbornú diskusiu.

Spolufinancované Európskou úniou prostredníctvom Programu Slovensko v rámci projektu č. NFP401101C360: Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom.

