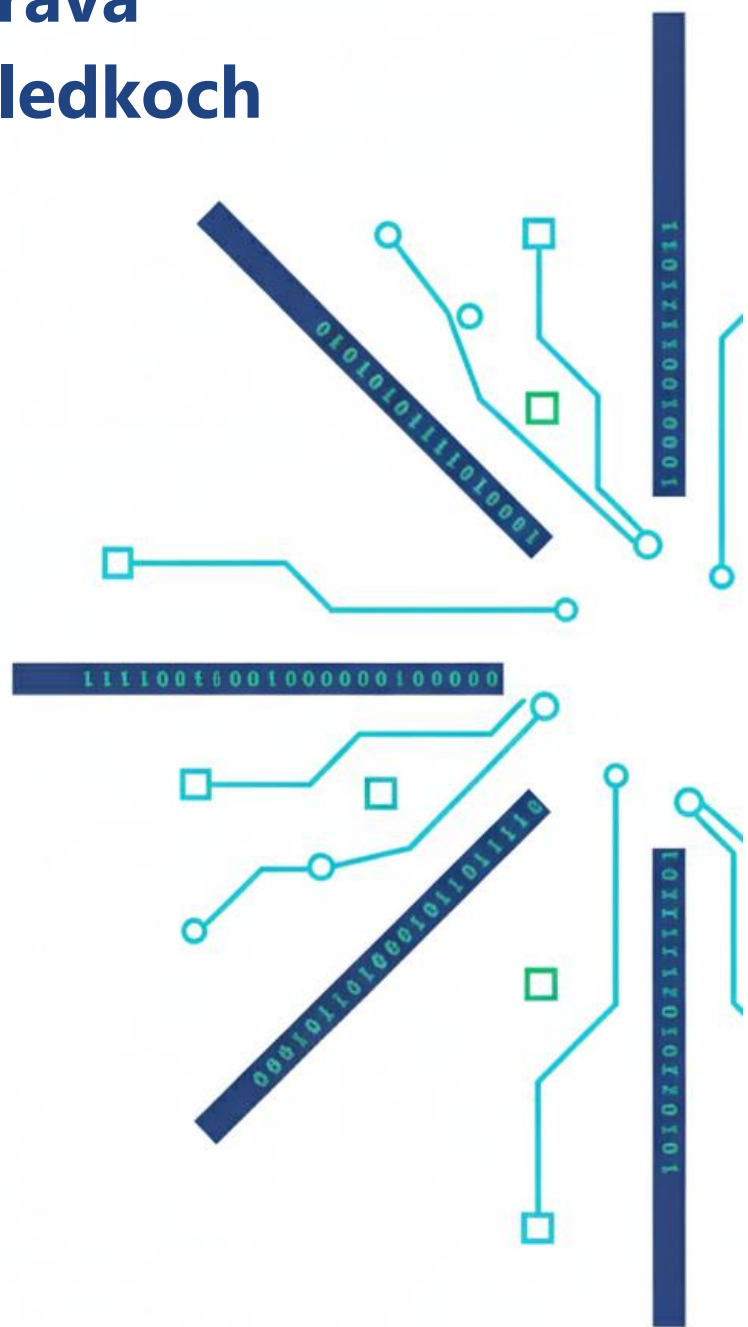


D06 - Závěrečná správa o dosiahnutých výsledkoch projektu ADFIR



Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Obsah

Obsah	1
Úvod.....	4
1 PhD. študenti, ktorých práce sú zamerané na problémy súvisiace s projektom ADFIR	6
1.1 Vymedzenie ukazovateľa	6
1.2 Analýza digitálnych stôp pomocou metód strojového učenia (Eva Marková)	6
1.3 Elektronické dôkazné prostriedky (Miroslav Srholec)	6
2 Spoločné projekty podporované inými schémami	8
2.1 Vymedzenie ukazovateľa	8
2.2 Prehľad projektov	8
2.3 Kompetenčné centrum kybernetickej bezpečnosti UPJŠ (17R05-04-V01-00007)	8
2.4 Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti (APVV-23-0137)	9
2.5 Právne, technické a forenzné aspekty kybernetickej bezpečnosti s prvkom umelej inteligencie (APVV-25-0162)	10
2.6 AI-driven cyber incident response technology (IstroSec s. r. o.)	11
2.7 Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom (401101C360)	12
3 Výskumné publikácie šíriace výsledky projektu	14
3.1 Vymedzenie ukazovateľa	14
3.2 Zoznam publikácií	14
3.2.1 Článok 1	14
3.2.2 Článok 2	14
3.2.3 Článok 3	15
3.2.4 Článok 4	15
3.2.5 Článok 5	16
4 Národné a medzinárodné spolupráce v akademickej sfére so štátnym aj súkromným sektorom	17
4.1 Vymedzenie ukazovateľa	17
4.2 Národné spolupráce	17
4.3 Medzinárodné spolupráce	18
5 Aktivity zamerané na šírenie výsledkov pre potenciálnych partnerov a zákazníkov	19

5.1	Vymedzenie ukazovateľa	19
5.2	Záverečná konferencia projektu ADFIR	19
5.3	Digitálna forenzná analýza - bezpečnosť AI (Košice)	19
5.4	Digitálna forenzná analýza - bezpečnosť AI (Rožňava)	20
5.5	Workshop - Digitálna forenzia v trestnom konaní: prax, úskalia a dôkazy	20
5.6	Workshop - Analýza údajov od teórie k praxi: analýza digitálnych stôp	21
5.7	Zaistovanie digitálnych stôp a ich použiteľnosť ako elektronických dôkazov v trestnom konaní	21
5.8	Prezentácia postera na konferencii DFRWS EU 2026	22
5.9	AI Community meetup	22
6	Publikované datasety a databázy	24
6.1	Vymedzenie ukazovateľa	24
6.2	Prehľad výstupov	24
6.3	D14 — Syntetický dataset	24
6.4	D22 — Databáza behaviorálnych vzorcov	25
7	Publikované metodológie	27
7.1	Vymedzenie ukazovateľa	27
7.2	Prehľad výstupov	27
7.3	D01 — Metodológia pre zmluvné vzťahy	27
7.4	D03 — Metodológia postupu spracovania digitálnych stôp	28
7.5	D23 — Metodológia pre tvorbu časovej osi prípadu	29
8	Publikované metódy a modely	31
8.1	Vymedzenie ukazovateľa	31
8.2	Prehľad výstupov	31
8.3	D02 — Metóda na anonymizáciu digitálnych stôp	32
8.4	D12 — Metóda na automatizovaný zber digitálnych stôp	33
8.5	D13 — Metóda na tvorbu datasetu	33
8.6	D15 — Model na extrakciu digitálnych stôp do maticovej reprezentácie	34
8.7	D16 — Model na extrakciu digitálnych stôp do grafovej reprezentácie	35
8.8	D17 — Model na agregáciu a prepojenie digitálnych stôp	36
8.9	D18 — Model na obohatenie digitálnych stôp	37
8.10	D19.1 — Metóda na identifikáciu digitálnych stôp: zhlukovanie a veľké jazykové modely	38
8.11	D19.2 — Metóda na identifikáciu digitálnych stôp: detekcia anomálií	38

8.12	<i>D20.1 — Metóda na identifikáciu vzťahov: faktorizácia formálneho kontextu</i>	39
8.13	<i>D20.2 — Metóda na identifikáciu vzťahov: významné časové okná</i>	40
8.14	<i>D21 — Metóda na určenie časového rámca a fáz útoku</i>	41
9	Ďalšie zverejnené výstupy projektu	43
9.1	<i>D24 — Rozšírená správa z forenznej analýzy</i>	43

Úvod

Projekt **Automatizácia digitálnej forenznej analýzy a odpovede na incident** (ďalej len „ADFIR“) je financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079. Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych dôkazov, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forenznych vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forenznych analytikov.** Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní.** Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné dôkazy pre vyšetrovanie a súdne konania.

Tento dokument (výstup D06 – Záverečná správa o dosiahnutých výsledkoch projektu) rozpisuje plnenie merateľných ukazovateľov projektu ADFIR. Pre každý ukazovateľ uvádza jeho vymedzenie, spôsob, akým bola stanovená cieľová hodnota, požiadavky na preukazovanie plnenia a konkrétne výsledky dosiahnuté v projekte. Služi ako podklad pre monitorovacie správy, ako aj ako prehľad pre riešiteľov projektu.

Súhrnný prehľad plnenia je uvedený v tabuľke č. 1. Podrobnosti ku každému ukazovateľu obsahujú jednotlivé kapitoly.

Očakávané výsledky a vplyv aktivít projektu	Očakávaný počet	Reálne plnenie
PhD. študenti, ktorých práce sú zamerané na problémy súvisiace s týmto projektom	2	2
Spoločné projekty podporované inými schémami	2	5

Očakávané výsledky a vplyv aktivít projektu	Očakávaný počet	Reálne plnenie
Výskumné publikácie šíriace výsledky projektu	4	5
Národné spolupráce v akademickej sfére a so štátnym aj súkromným sektorom	2	3
Medzinárodné spolupráce v akademickej sfére a so štátnym aj súkromným sektorom	2	3
Aktivity zamerané na šírenie výsledkov pre potenciálnych partnerov/zákazníkov	3	7
Publikované datasety a databázy	2	2
Publikované metodológie	3	3
Publikované metódy a modely	10	12

Tabuľka č. 1 – Očakávanie výsledky a vplyv aktivít projektu

Kapitoly 6 až 8 tejto správy obsahujú podrobný popis jednotlivých publikovaných datasetov a databáz, metodológií a metód a modelov vrátane zhrnutia ich obsahu, použitých technológií, dosiahnutých výsledkov a väzby na špecifické ciele projektu. Ku každému výstupu je uvedený aj názov dokumentu, v ktorom je výstup podrobne opísaný.

1 PhD. študenti, ktorých práce sú zamerané na problémy súvisiace s projektom ADFIR

Očakávaný počet	Reálne plnenie	Stav
2	2	Splnené

1.1 Vymedzenie ukazovateľa

Základom pre odhad tohto ukazovateľa boli aktuálne a plánované doktorandské pozície, ktorých témy odrážajú problémy definované v projekte ADFIR. Ukazovateľ sleduje budovanie výskumnej kapacity v oblasti automatizovanej digitálnej forenzej analýzy.

1.2 Analýza digitálnych stôp pomocou metód strojového učenia (Eva Marková)

Údaj	Hodnota
Téma dizertačnej práce	Analýza digitálnych stôp pomocou metód strojového učenia
Študentka	RNDr. Eva Marková
Pracovisko	Ústav informatiky, Prírodovedecká fakulta UPJŠ v Košiciach
Školiteľ	doc. JUDr. RNDr. Pavol Sokol, PhD. et PhD.
Podporná dokumentácia	Eva_Marková_zadanie_záverečnej_práce_SK_EN

Väzba na projekt: téma priamo napĺňa vecné jadro pracovných balíkov KPB3 a KPB4 - reprezentáciu digitálnych stôp a ich analýzu metódami strojového učenia. Doktorandka je spoluautorkou publikačného výstupu projektu prezentovaného na konferencii ARES 2025.

1.3 Elektronické dôkazné prostriedky (Miroslav Srholec)

Údaj	Hodnota
Téma dizertačnej práce	Elektronické dôkazné prostriedky
Študent	JUDr. Miroslav Srholec, PhD.
Pracovisko	Univerzita Pavla Jozefa Šafárika v Košiciach

Údaj	Hodnota
Školiteľ	prof. JUDr. Sergej Romža, PhD.
Podporná dokumentácia	Miroslav_Srholec_zadanie_záverečnej_práce_SK_EN https://www.upjs.sk/app/uploads/sites/11/2025/07/oznam_Srholec.pdf

Väzba na projekt: téma pokrýva právnu vetvu projektu riešenú v pracovnom balíku KPB1, teda prípustnosť a dôkaznú použiteľnosť výstupov automatizovanej forenznej analýzy v trestnom konaní.

2 Spoločné projekty podporované inými schémami

Očakávaný počet	Reálne plnenie	Stav
2	5	Prekročené

2.1 Vymedzenie ukazovateľa

Základom pre odhad boli prebiehajúce a plánované návrhy projektov, ktoré sa týkajú problémov riešených v projekte ADFIR.

2.2 Prehľad projektov

Č.	Projekt	Riešiteľ	Stav
1	Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (17R05-04-V01-00007)	UPJŠ	Realizovaný
2	Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti (APVV-23-0137)	UPJŠ	Realizovaný
3	Právne, technické a forenzné aspekty kybernetickej bezpečnosti s prvkom umelej inteligencie (APVV-25-0162)	UPJŠ	Podaný
4	AI-driven cyber incident response technology (09I05-03-V03-00005)	IstroSec s. r. o.	Realizovaný
5	Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom (401101C360)	IstroSec s. r. o.	Realizovaný

2.3 Kompetenčné centrum kybernetickej bezpečnosti UPJŠ (17R05-04-V01-00007)

Údaj	Hodnota
Kód projektu	17R05-04-V01-00007
Schéma	Plán obnovy a odolnosti SR, komponent 17 – Digitálne Slovensko

Údaj	Hodnota
Prijímateľ	Univerzita Pavla Jozefa Šafárika v Košiciach
Trvanie projektu	január 2025 – marec 2026
Celkové oprávnené výdavky	1 585 417,19 EUR s DPH
Miesto realizácie	Univerzita Pavla Jozefa Šafárika v Košiciach a jej odborné pracoviská

Cieľ a anotácia: Cieľom projektu je vytvorenie Kompetenčného centra kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ). V rámci kompetenčného centra sú realizované povinné aj nepovinné aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. KC KB UPJŠ zároveň realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti. Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti — potrebu zvýšiť bezpečnostné povedomie relevantných subjektov, najmä zamestnancov verejnej správy a študentov vysokých a stredných škôl, vzdelávať a vychovávať nových odborníkov, skúmať kybernetické hrozby a identifikovať adekvátne reakcie na ne a zvýšiť operatívnu bezpečnosť vo verejnej správe poskytovaním expertných činností zo strany CSIRT tímu. Výstupmi projektu sú najmä študijný plán magisterského stupňa študijného programu aplikovaná informatika so zameraním na kybernetickú bezpečnosť a súvisiace nové alebo modifikované predmety, ponuka vzdelávania pre rôzne cieľové skupiny zamestnancov verejnej správy, posilnená spolupráca so strednými školami prostredníctvom činnosti KyberTímov, odporúčania pre verejnú správu v rôznych oblastiach kybernetickej a informačnej bezpečnosti, kampane zamerané na zvyšovanie bezpečnostného povedomia, vedecké publikácie a nové výskumné spolupráce, ako aj doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu s možnosťou poskytovania expertných činností pre akreditované CSIRT tímy v SR.

Súvislosť s projektom ADFIR: Kompetenčné centrum vytvára inštitucionálne a personálne zázemie pre výskum v oblasti kybernetickej a informačnej bezpečnosti a digitálnej forenzej analýzy na UPJŠ a prekrýva sa s riešiteľskou základňou projektu ADFIR. Univerzitný CSIRT tím a vzdelávacie aktivity kompetenčného centra zároveň predstavujú prirodzený kanál pre prenos výsledkov projektu ADFIR do praxe riešenia incidentov a do výučby.

2.4 Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti (APVV-23-0137)

Údaj	Hodnota
Číslo projektu	APVV-23-0137
Schéma	Agentúra na podporu výskumu a vývoja — všeobecná výzva
Zodpovedná organizácia	Univerzita Pavla Jozefa Šafárika v Košiciach
Odkaz	https://portal.ccvapp.upjs.sk/project-view/2810
Stav	V realizácii

Cieľ a anotácia: Situačné povedomie o kybernetickej bezpečnosti, ktoré v sebe zahŕňa zber a uchovávanie bezpečnostných údajov, ich analýzu a zdieľanie, ako aj ich predikciu, so sebou prináša mnoho právnych aj technických výziev, ktoré je potrebné skúmať vo vzájomnej synergii. Riešiteľský kolektív zložený z odborníkov z vybraných oblastí práva a technických smerov si kladie za cieľ vykonať analýzu súčasnej právnej úpravy týkajúcej sa situačného povedomia s ohľadom na zber, uloženie a zdieľanie bezpečnostných údajov, ako aj analýzu právnej úpravy s ohľadom na použitie jednotlivých metód strojového učenia pre analýzu bezpečnostných údajov a predikciu situačného povedomia. Unikátnym výstupom projektu budú odporúčania pre povinné subjekty v zmysle právnej úpravy kybernetickej bezpečnosti, technický spôsob zbierania bezpečnostných údajov s ohľadom na právne aspekty a návrh a implementácia metód strojového učenia pre identifikáciu relevantných bezpečnostných údajov a pre predikciu situačného povedomia.

Súvislosť s projektom ADFIR: Projekt zdieľa s projektom ADFIR metodické jadro - prepojenie právnej analýzy s dátovou analýzou a strojovým učením nad bezpečnostnými údajmi. Zatiaľ čo ADFIR sa zameriava na digitálne stopy a forenznú analýzu po incidente, tento projekt rieši situačné povedomie pred incidentom a počas neho. Prekrýva sa aj riešiteľská základňa oboch projektov.

2.5 Právne, technické a forenzné aspekty kybernetickej bezpečnosti s prvkom umelej inteligencie (APVV-25-0162)

Údaj	Hodnota
Číslo projektu	APVV-25-0162
Schéma	Agentúra na podporu výskumu a vývoja
Zodpovedný riešiteľ	prof. JUDr. Jozef Čentéš, DrSc.
Odbor výskumu	050509 – Trestné právo

Údaj	Hodnota
Realizácia	2026 – 2030
Stav	Schválený projektový návrh

Anotácia a cieľ: Rozvoj umelej inteligencie zásadne mení charakter kybernetických bezpečnostných rizík a incidentov. Systémy umelej inteligencie sa stávajú integrálnou súčasťou kritických procesov verejnej správy, hospodárstva a kritickej infraštruktúry, čím vznikajú nové typy kybernetických bezpečnostných incidentov. Tieto incidenty sa vyznačujú vysokou mierou automatizácie, adaptivity a schopnosťou generovať špecifické digitálne artefakty, ktoré sa zásadne odlišujú od tradičných elektronických dôkazov. Súčasné právne, metodické a forenzné rámce však tieto špecifiká reflektujú len čiastočne. Cieľom projektu je vytvoriť aplikačne využiteľný právno-technický a kriminalisticko-forenzný rámec pre identifikáciu, analýzu a riešenie kybernetických bezpečnostných incidentov s prvkom umelej inteligencie. Projekt sa zameriava na systematickú identifikáciu a klasifikáciu incidentov alebo porúch systémov umelej inteligencie vrátane kybernetických bezpečnostných incidentov s prvkom umelej inteligencie („AI incidenty“), ako aj na návrh metodiky práce s digitálnymi stopami vznikajúcimi alebo ovplyvnenými činnosťou systémov umelej inteligencie („AI stopy“). Projekt je koncipovaný ako aplikovaný interdisciplinárny výskum, ktorý prepája trestné právo, kybernetickú bezpečnosť a digitálnu forenznú činnosť. Využíva doktrínalnu a komparatívnu právnu analýzu, kriminalisticko-forenzné metódy a empirický výskum realizovaný v spolupráci s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti a CSIRT jednotkami. Očakávané výstupy budú mať charakter metodických, analytických a odporúčacích dokumentov priamo využiteľných v praxi, najmä pri metodickej podpore subjektov verejnej správy, riešení kybernetických incidentov a spolupráci s orgánmi činnými v trestnom konaní. Projekt prispeje k zvýšeniu kybernetickej odolnosti štátu, k posilneniu právnej istoty a k lepšej integrácii právnych a technických nástrojov pri riešení hrozieb spojených s umelou inteligenciou.

Súvislosť s projektom ADFIR: Projektový návrh priamo nadväzuje na výsledky projektu ADFIR a rozširuje ich o aspekty umelej inteligencie vo forenznej analýze. Kým ADFIR vytvoril metódy automatizovanej analýzy digitálnych stôp a právny rámec ich použiteľnosti v trestnom konaní, nadväzujúci projekt sa zameriava na novú kategóriu stôp vznikajúcich činnosťou systémov umelej inteligencie a na incidenty, ktorých sú tieto systémy súčasťou.

2.6 AI-driven cyber incident response technology (IstroSec s. r. o.)

Údaj	Hodnota
Číslo projektu	09I05-03-V03-00005
Prijímateľ	IstroSec s. r. o.
Schéma	Plán obnovy a odolnosti Slovenskej republiky, Investícia 5

Údaj	Hodnota
Termín realizácie	11/2024 – 03/2026
Oprávnené výdavky	1 181 314,51 EUR, z toho prostriedky mechanizmu 792 613,07 EUR
Miesto realizácie	Vajnorská 100/B, 831 04 Bratislava 3
Odkaz	https://istrosec.com/sk/eu-projects/ai-driven-cyber-incident-response-technology/

Cieľ: Cieľom projektu je vyskúmať a vyvinúť pokročilú technológiu poháňanú umelou inteligenciou na detekciu a riešenie kybernetických incidentov s cieľom automatizácie procesov a samostatného učenia sa modelov umelej inteligencie. Projekt je zameraný na výskum a vývoj pokročilého nástroja na analýzu hrozieb a prediktívnu analýzu a predstavuje výrazný posun v oblasti inovácií kybernetickej bezpečnosti.

Súvislosť s projektom ADFIR: Predmetný projekt rieši automatizáciu reakcie na kybernetické incidenty metódami umelej inteligencie, čo vecne zodpovedá pracovným balíkom KPB2 a KPB4 projektu ADFIR, teda zberu digitálnych stôp a ich analýze. Partner IstroSec tak môže výsledky projektu ADFIR priamo prenášať do vývoja komerčného nástroja na riešenie incidentov.

2.7 Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom (401101C360)

Údaj	Hodnota
Kód projektu	401101C360
Výzva	SVaV – Strategický výskum a vývoj prostredníctvom partnerstiev (PSK-MSVVM-020-2024-DV-EFRR)
Schéma	Program Slovensko
Prijímateľ	Žilinská univerzita v Žiline
Partneri	IstroSec s. r. o., Syteli s. r. o., Technická univerzita v Košiciach
Termín realizácie	04/2026 – 10/2029
Oprávnené výdavky pre IstroSec	3 470 896,45 EUR, z toho nenávratný finančný príspevok 2 776 717,16 EUR

Údaj	Hodnota
Miesto realizácie	Žilina
Webová stránka projektu	https://www.cybersecurityresearch.sk
Odkaz	https://istrosec.com/sk/eu-projects/vyskum-a-vyvoj-ai-na-detekciu-kybernetickych-hrozieb-a-obranu-proti-utokom/

Cieľ: Cieľom projektu je výskum pokročilých metód detekcie, ktoré integrujú umelú inteligenciu a behaviorálne modely, čím zásadne rozširujú súčasný stav techniky. Projekt je zameraný na mapovanie aktuálnych hrozieb, výskum metód analýzy správania útočníkov a testovanie bezpečnostných opatrení v realistických podmienkach.

Súvislosť s projektom ADFIR: Výskum metód analýzy správania útočníkov priamo nadväzuje na pracovný balík KPB4 projektu ADFIR, najmä na identifikáciu behaviorálnych vzorcov a na databázu behaviorálnych vzorcov (výstup D22). Projekt zároveň rozširuje spoluprácu partnera IstroSec o ďalšie slovenské výskumné inštitúcie.

3 Výskumné publikácie šíriace výsledky projektu

Očakávaný počet	Reálne plnenie	Stav
4	5	Prekročené

3.1 Vymedzenie ukazovateľa

Základom pre odhad bol počet predchádzajúcich vedeckých článkov publikovaných kľúčovými členmi výskumného tímu. Ukazovateľ zahŕňa recenzované publikácie, ktoré šíria výsledky projektu v odbornej komunite. Publikácie sú výstupom D25 - Recenzované vedecké články.

3.2 Zoznam publikácií

3.2.1 Článok 1

Hennelová, Z., Marková, E., & Sokol, P. (2025). **The Impact of Anti-forensic Techniques on Data-Driven Digital Forensics: Anomaly Detection Case Study**. In International Conference on Availability, Reliability and Security (ARES 2025), Lecture Notes in Computer Science (pp. 131–148). Cham: Springer Nature Switzerland.

Odkaz na článok: https://link.springer.com/chapter/10.1007/978-3-032-00635-6_8

Abstrakt: Digitálna forenzná analýza má zásadný význam pri reakcii na kybernetické hrozby a incidenty, pretože umožňuje vyšetrovateľom identifikovať, zbierať a analyzovať digitálne dôkazy. S rastúcou sofistikovanosťou útokov útočníci využívajú anti-forenzné techniky na obchádzanie detekcie a sťažovanie forenzného vyšetrovania. Tieto techniky sa usilujú odstrániť, zahmlieť alebo manipulovať digitálne stopy, čím znižujú účinnosť forenznej analýzy. Napriek rastúcemu záujmu o anti-forenzné techniky sa doteraz venovalo len obmedzené úsilie systematickému hodnoteniu jej reálneho dopadu. V príspevku sa skúmajú účinky vybraných anti-forenzných techník — vymazania súborov a záznamov, ukrývania údajov v alternatívnych dátových prúdoch, šifrovania, vytvárania falošných dôkazov a manipulácie s časovými pečiatkami — na dva kľúčové aspekty: na integritu a dostupnosť digitálnych stôp a na presnosť algoritmickej detekcie anomálií v dátovo riadenej forenznej analýze.

3.2.2 Článok 2

Hennelová, Z., Sokol, P., Bajtoš, T., & Krišáková, S. P. (2025). **Data-Driven Digital Forensics: Anomaly Detection in Mozilla Firefox**. In ITAT 2025: Information Technologies — Applications and Theory (pp. 404–413). CEUR Workshop Proceedings, Vol. 4092.

Odkaz na článok: <https://ceur-ws.org/Vol-4092/paper33.pdf>

Abstrakt: Používanie webových prehliadačov generuje veľké množstvo údajov, ktoré môžu slúžiť ako hodnotné forenzné artefakty pri vyšetrowaní kybernetických incidentov. Tieto artefakty obsahujú informácie o navštívených stránkach, stiahnutých súboroch a časových pečiatkach používateľskej aktivity, ktoré pomáhajú identifikovať vektor útoku. Existujúce nástroje umožňujú tieto údaje vizualizovať, ich vyhodnotenie je však časovo náročné a výrazne závisí od skúseností analytika. Príspevok využíva metodiku dátovo riadenej digitálnej forenzej analýzy s cieľom automatizovať identifikáciu podozrivých udalostí pomocou algoritmov strojového učenia. Údaje z prehliadača Mozilla Firefox sa spracúvajú do jednotnej časovej osi, nad ktorou sa detegujú anomálie. Výsledky ukazujú, že metódy ECOD a COPOD predstavujú vhodný kompromis medzi presnosťou a objemom výstupných údajov.

3.2.3 Článok 3

Antoni, L., Sokol, P., Krišáková, S. P., Kotlárová, D., Krídlo, O., & Krajči, S. (2025). **Formal Concept Analysis and Attribute Dependencies of NIST Data Leakage Case**. In ITAT 2025: Information Technologies — Applications and Theory (pp. 358–368). CEUR Workshop Proceedings, Vol. 4092.

Odkaz na článok: <https://ceur-ws.org/Vol-4092/paper29.pdf>

Abstrakt: Bezpečnostné incidenty spojené s neoprávneným prístupom a únikom údajov zostávajú jednou z najkritickejších výziev súčasnej kybernetickej bezpečnosti a vyžadujú transparentné a interpretovateľné metódy analýzy správania. Príspevok predstavuje aplikáciu formálnej konceptovej analýzy a dolovania asociačných pravidiel na dátovú sadu NIST Data Leakage Case EVT, ktorá simuluje bezpečnostný incident s možnou exfiltráciou údajov. Cieľom je odhaliť a interpretovať logické závislosti medzi binárnymi auditnými atribútmi a časovými črtami extrahovanými zo systémových záznamov. Autori konštruujú konceptuálny vzťah s 26 formálnymi konceptmi nad dátovou sadou s 10 306 riadkami a 11 atribútmi, odvodzujú kanonickú bázu atribútových implikácií so 100 % spoľahlivosťou a rozširujú ju o približné asociačné pravidlá. Výsledky poukazujú na typické konfigurácie prístupu aj na anomálne kombinácie zahŕňajúce víkendovú a nočnú aktivitu.

3.2.4 Článok 4

Bača, M., Krišáková, S. P., & Sokol, P. (2026). **Identification of Relevant Digital Forensic Traces Using Time Window Aggregation and Hierarchical Clustering**. In International Conference on Computational Intelligence in Security for Information Systems (CISIS 2026), Communications in Computer and Information Science (pp. 224–236). Cham: Springer Nature Switzerland.

Abstrakt: Digitálne forenzné vyšetrowania čelia čoraz častejšie výzve analyzovať veľké objemy heterogénnych údajov, pričom identifikácia relevantných digitálnych stôp zostáva zložitou a na zdroje náročnou úlohou. Príspevok navrhuje metodiku systematickej identifikácie relevantných forenzných artefaktov založenú na agregácii do časových okien a na hierarchickom zhľukovaní. Navrhovaný prístup zavádza kvantitatívne metriky, ako sú attack rate a attack lift, na hodnotenie relevantnosti zhľukov a zároveň kladie dôraz

na vysvetliteľnosť prostredníctvom identifikácie kľúčových atribútov, ktoré jednotlivé zhľuky charakterizujú. Metodika bola overená na viacerých verejne dostupných dátových sadách; výsledky ukazujú, že prístup účinne podporuje identifikáciu správania súvisiaceho s incidentom pri zachovaní interpretovateľnosti.

3.2.5 Článok 5

Kordík, M. (2026). **Outline of Principles for the Analysis of Open-Source Intelligence (OSINT) as Evidence in Criminal Proceedings**. Acta Facultatis Iuridicae Universitatis Comenianae, 45(2), s. 3–16.

Odkaz na článok: <https://afi.flaw.uniba.sk/index.php/AFI/en/article/view/1478>

Abstrakt: Článok sa zaoberá možnosťou využitia analýzy otvorených zdrojov ako dôkazu v trestnom konaní a snaží sa vymedziť minimálne štandardy na jeho použitie tak, aby boli naplnené požiadavky Trestného poriadku, a to v pozitívnom zmysle princípov aj princípov vymedzených negatívne. Príspevok sa vysporiadava s používanou terminológiou v tejto oblasti a analyzuje pripravovanú úpravu zmeny zaistovania elektronických dôkazov, ktorá však z tohto pohľadu neprináša relevantnú zmenu. Pri argumentácii čerpá z rozhodovacej činnosti Medzinárodného trestného súdu a poskytuje výklad noriem Budapeštianskeho dohovoru pre možnosť zdieľania OSINT analýzy ako jedného zo základných prameňov pre zdieľanie digitálnych dôkazov v Európe. Autor rozlišuje negatívne princípy — zákaz prekonania odporu a zákaz infiltrácie do uzavretých skupín — a pozitívne princípy nevyhnutnosti, identifikácie, objektivity a absencie konfliktu záujmov, podpornej funkcie a bezpečnosti OSINT postupov.

4 Národné a medzinárodné spolupráce v akademickej sfére so štátnym aj súkromným sektorom

Typ spolupráce	Očakávaný počet	Reálne plnenie	Stav
Národné spolupráce	2	3	Prekročené
Medzinárodné spolupráce	2	3	Prekročené

4.1 Vymedzenie ukazovateľa

Základom pre odhad boli už existujúce spolupráce a potenciál pre budúce spolupráce s entitami, ktoré majú prirodzený záujem o výsledky projektu. Pri existujúcich partnerstvách sú uvedené zmluvy s odkazom na Centrálny register zmlúv spolu s odôvodnením súvislosti. V prípade potenciálnych nových spoluprác sú uvedené Potvrdenia o záujme spolupracovať.

4.2 Národné spolupráce

Organizácia	Forma	Odkaz
DISIG, a. s.	Zmluva o spolupráci	https://www.crz.gov.sk/zmluva/7377499/
ESET, spol. s r. o.	Zmluva o spolupráci	https://www.crz.gov.sk/zmluva/8052347/
Binary Confidence s. r. o.	Potvrdenie o záujme spolupracovať	Letter_of_intent_Binary_confidence

DISIG, a. s. je slovenská spoločnosť pôsobiaca v oblasti dôveryhodných služieb a informačnej bezpečnosti. Predmetom spolupráce je výskum a aplikácia strojového učenia v rámci identifikácie relevantných záznamov v systémoch SIEM. Spolupráca priamo nadväzuje na pracovný balík KPB4, teda na identifikáciu relevantných digitálnych stôp metódami strojového učenia.

ESET, spol. s r. o. je globálna spoločnosť pôsobiaca v oblasti kybernetickej bezpečnosti so sídlom na Slovensku. Predmetom spolupráce je využitie vedeckých kapacít Prírodovedeckej fakulty UPJŠ pri výskume v oblasti integrácie dátovej analýzy a strojového učenia do činností tímov SOC. Spolupráca prepája výsledky projektu s prevádzkou bezpečnostných dohľadových centier.

Binary Confidence s. r. o. je slovenská spoločnosť poskytujúca služby monitorovania a riešenia kybernetických bezpečnostných incidentov. Ako prevádzkovateľ bezpečnostného

dohľadového centra predstavuje prirodzeného používateľa výsledkov projektu v oblasti automatizácie forenznej analýzy.

4.3 Medzinárodné spolupráce

Organizácia	Krajina	Forma
Axenta a. s.	Česká republika	Letter_of_intent_Axenta_CZ
The Science, Entrepreneurship and Technologies University (SET)	Ukrajina	Letter_of_Intent_SET
Universidad de Málaga	Španielsko	Letter_of_intent_University_Malaga

Axenta a. s. je česká spoločnosť špecializujúca sa na kybernetickú bezpečnosť a prevádzku bezpečnostných dohľadových centier. Spolupráca umožňuje overenie prenositeľnosti výsledkov projektu do prostredia českého trhu a do praxe komerčných tímov reakcie na incidenty.

The Science, Entrepreneurship and Technologies University (SET) je ukrajinská vysoká škola. Spolupráca prináša do projektu perspektívu prostredia s vysokou intenzitou kybernetických útokov a rozširuje medzinárodný dosah výsledkov projektu.

Universidad de Málaga je španielska verejná univerzita s výskumným zázemím v oblasti kybernetickej bezpečnosti a formálnych metód analýzy údajov. Spolupráca je komplementárna najmä k metódam formálnej konceptuálnej analýzy uplatneným v pracovnom balíku KPB4.

5 Aktivity zamerané na šírenie výsledkov pre potenciálnych partnerov a zákazníkov

Očakávaný počet	Reálne plnenie	Stav
3	7	Prekročené

5.1 Vymedzenie ukazovateľa

Základom pre odhad boli plánované aktivity na šírenie výsledkov v rámci projektu, teda konferencie a workshopy. Aktivity naplňajú výstupy pracovného balíka KPB5, a to D26 — Workshop pre študentov a D27 — Workshop pre potenciálne zainteresované strany. Celkovo bolo zrealizovaných sedem aktivít oproti trom plánovaným, pričom cieľové skupiny zahŕňali stredoškolákov, vysokoškolských študentov informatiky a práva, advokátov a odbornú verejnosť z akademického prostredia, verejnej správy a bezpečnostných spoločností.

5.2 Záverečná konferencia projektu ADFIR

Údaj	Hodnota
Dátum	24. jún 2026
Miesto	Amfiteáter, 2. poschodie starej budovy, Právnická fakulta Univerzity Komenského v Bratislave
Partneri	UPJŠ, EISI, IstroSec
Počet účastníkov	31
Typ účastníkov	odborná verejnosť

Odkaz: <https://adfir.upjs.sk/2026/06/17/zaverecna-konferencia-projektu-adfir/>

Anotácia: Záverečná konferencia bola venovaná prezentácii výsledkov projektu ADFIR a odbornej diskusii o automatizácii digitálnej forenznej analýzy, jej právnych limitoch a možnostiach využitia nielen v trestnom konaní. Na organizácii sa podieľali všetci traja partneri projektu a podujatie svojím zameraním prepojilo technickú, výskumnú a právnu rovinu projektu. Konferencia bola realizovaná nad rámec výstupu D27 a vykazuje sa ako samostatná diseminačná aktivita.

5.3 Digitálna forezná analýza - bezpečnosť AI (Košice)

Údaj	Hodnota
Dátum	3. november 2025
Miesto	Prírodovedecká fakulta UPJŠ v Košiciach, Park Angelinum 9, Košice
Školiteľ / prednášajúci	Mgr. Sophia Petra Krišáková
Počet účastníkov	17
Typ účastníkov	stredoškoly

Anotácia: Vzdelávacia aktivita pre stredoškolských študentov predstavujúca základy digitálnej forenzej analýzy a bezpečnostné aspekty umelej inteligencie. Aktivita napĺňa cieľ projektu smerujúci k popularizácii témy medzi budúcimi odborníkmi.

5.4 Digitálna forenzná analýza - bezpečnosť AI (Rožňava)

Údaj	Hodnota
Dátum	23. február 2026
Miesto	Stredná odborná škola technická, Hviezdoslavova 5, Rožňava
Školiteľ / prednášajúci	Mgr. Sophia Petra Krišáková
Počet účastníkov	37
Typ účastníkov	stredoškoly

Anotácia: Opakovanie vzdelávacej aktivity na strednej odbornej škole technickej s rozšíreným záberom účastníkov. Aktivita rozširuje geografický dosah projektu mimo krajské mesto.

5.5 Workshop - Digitálna forenzia v trestnom konaní: prax, úskalia a dôkazy

Údaj	Hodnota
Dátum	4. máj 2026
Miesto	Prírodovedecká fakulta UPJŠ v Košiciach, Jesenná 5, Košice

Údaj	Hodnota
Školiteľ / prednášajúci	Ing. Jaroslav Oster
Počet účastníkov	20
Typ účastníkov	študenti vysokej školy (informatika a právo)

Anotácia: Interdisciplinárny workshop spájajúci študentov informatiky a práva, zameraný na praktické úskalia zaistovania a interpretácie digitálnych stôp a na ich použiteľnosť ako dôkazu v trestnom konaní.

5.6 Workshop - Analýza údajov od teórie k praxi: analýza digitálnych stôp

Údaj	Hodnota
Dátum	13. november 2025
Miesto	Prírodovedecká fakulta UPJŠ v Košiciach, Jesenná 5, Košice
Školiteľ / prednášajúci	Mgr. Sophia Petra Krišáková
Počet účastníkov	približne 10
Typ účastníkov	študenti vysokej školy (informatika)

Anotácia: Praktický workshop pre študentov informatiky venovaný postupu od teoretických základov dátovej analýzy k aplikácii na reálne digitálne stopy.

5.7 Zaistovanie digitálnych stôp a ich použiteľnosť ako elektronických dôkazov v trestnom konaní

Údaj	Hodnota
Dátum	24. júna 2026, 10:00 – 12:00
Miesto	Budova Slovenskej advokátskej komory, Kolárska 6148/4, Bratislava
Školiteľ / prednášajúci	doc. JUDr. Marek Kordík, LL.M., PhD., JUDr. Petra Dražová, doc. RNDr. JUDr. Pavol Sokol, PhD. et PhD.

Údaj	Hodnota
Počet účastníkov	20
Typ účastníkov	advokáti

Anotácia: Odborné podujatie pre advokátov realizované v spolupráci so Slovenskou advokátskou komorou. Zameriavalo sa na zaistovanie digitálnych stôp a na podmienky ich prípustnosti ako elektronických dôkazov. Podujatie priamo napĺňa cieľ projektu smerujúci k akceptácii nového metodického prístupu k analýze digitálnych dôkazov právnickými profesiami a ako jedna z troch kľúčových aktivít pre potenciálnych používateľov výsledkov napĺňa referenčný ukazovateľ projektu.

5.8 Prezentácia postera na konferencii DFRWS EU 2026

Údaj	Hodnota
Dátum	23. – 27. marec 2026
Miesto	Linköping University (LiU)
Školiteľ / prednášajúci	Sophia Petra Krišáková, Pavol Sokol, Martin Bača, Radovan Slíž, Matej Mikuláš
Počet účastníkov	približne 200 účastníkov konferencie
Typ účastníkov	odborná verejnosť z akademického prostredia a verejnej správy, zástupcovia bezpečnostných spoločností

Názov posteru: Lifecycle of Automated Digital Forensic Analysis Using Machine Learning.

Anotácia: Poster predstavil ucelený životný cyklus automatizovanej digitálnej forenznej analýzy s využitím strojového učenia, tak ako ho projekt ADFIR pokrýva naprieč pracovnými balíkmi KPB2 až KPB5. Podujatie umožnilo prezentovať výsledky projektu pred medzinárodnou komunitou digitálnej forenznej analýzy.

5.9 AI Community meetup

Údaj	Hodnota
Dátum	18. jún 2026, 8:30 – 10:30
Miesto	Univerzitný vedecký park TECHNICOM, Němcovej 5, Košice

Údaj	Hodnota
Školiteľ / prednášajúci	Košice IT Valley v spolupráci s UPJŠ
Počet účastníkov	26
Typ účastníkov	IT profesionáli, bezpečnostní experti, výskumníci, študenti

Odkaz: <https://www.kosiceitvalley.sk/events/ai-community-meetup/>

Anotácia: Druhé stretnutie komunity zaoberajúcej sa umelou inteligenciou v Košiciach, venované prepojeniu umelej inteligencie, strojového učenia a kybernetickej bezpečnosti. Program bol zameraný na to, ako umelá inteligencia pomáha pri detekcii incidentov, automatizácii bezpečnostných procesov a digitálnej forenznej analýze. V rámci podujatia bol predstavený projekt ADFIR a jeho výskumné a inovačné výsledky v oblasti automatizácie reakcie na kybernetické incidenty. Podujatie bolo určené IT profesionálom, bezpečnostným expertom, výskumníkom a študentom a jeho cieľom bolo aj nadviazanie kontaktov medzi akademickým a firemným prostredím. Účasť bola bezplatná s povinnou registráciou pri obmedzenej kapacite.

6 Publikované datasety a databázy

Očakávaný počet	Reálne plnenie	Stav
2	2	Splnené

6.1 Vymedzenie ukazovateľa

Základom pre odhad bol počet datasetov a databáz, ktoré je potrebné pripraviť na dosiahnutie cieľov projektu. Do ukazovateľa spadajú výstupy typu „dataset“ a „databáza“ určené na zverejnenie. Ide o dva výstupy pokrývajúce dve odlišné vrstvy dátového reťazca projektu: vstupné forenzné údaje pre tréning a porovnávanie metód (D14) a znalostnú bázu vzorcov správania útočníka získanú analýzou (D22).

6.2 Prehľad výstupov

Číslo	Výstup	Pracovný balík	Zodpovedný partner	Prístup
D14	Syntetický dataset	KPB2	UPJŠ	Verejný
D22	Databáza behaviorálnych vzorcov	KPB4	IstroSec	Verejný

6.3 D14 — Syntetický dataset

Údaj	Hodnota
Číslo výstupu	D14
Pracovný balík / úloha	KPB2, úloha KPB2.3
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	dataset
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D14-KPB2-03-Synteticky-dataset (SK)

Zhrnutie: Výstupom je syntetický forenzný dataset vytvorený pre potreby porovnávania metód analýzy digitálnych stôp. Riešiteľský tím vychádzal zo zistenia, že v oblasti digitálnej forenznej analýzy neexistuje dátová sada použiteľná na všetky výskumné účely a že existujúce

sady buď nie sú zdieľané, alebo im chýba dokumentácia a formálny popis konštrukcie. Dataset bol preto vytvorený predovšetkým z dátových sád používaných v súťažiach Capture The Flag a primerane doplnený realistickými údajmi tak, aby opisoval scenáre, ktoré sa môžu vyskytnúť v skutočných bezpečnostných incidentoch. Súčasťou výstupu je úplná dokumentácia postupu konštrukcie datasetu, popis zahrnutých artefaktov a vymedzenie jeho limitov — riešiteľský tím výslovne uvádza, že takáto dátová sada nemusí pokrývať všetky situácie, ktoré môžu v reálnom prostredí nastať. Dataset pokrýva artefakty operačného systému Windows vrátane súborového systému NTFS a je pripravený v štruktúre vhodnej pre nadväzujúce spracovanie v pracovnom balíku KPB3.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu — identifikáciu potenciálnych zdrojov forenzných artefaktov, ich zber a identifikáciu vhodnej reprezentácie. Dataset tvorí vstupnú dátovú základňu pre modely reprezentácie v pracovnom balíku KPB3 a pre analytické metódy v pracovnom balíku KPB4.

6.4 D22 — Databáza behaviorálnych vzorcov

Údaj	Hodnota
Číslo výstupu	D22
Pracovný balík / úloha	KPB4, úloha KPB4.4
Zodpovedný partner	IstroSec s. r. o.
Typ	databáza
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D22-KPB4-04-Databaza-behavioralnych-vzorcov (SK)

Zhrnutie: Výstupom je katalóg detekčných pravidiel, v ktorom každé pravidlo opisuje jednu konkrétnu, pozorovateľnú stopu útočnickej aktivity. Pravidlá sú postavené nad tromi typmi telemetrie: udalosťami vytvorenia procesu (typicky Event ID 4688, Sysmon Event ID 1 alebo telemetria EDR), záznamami v protokoloch udalostí Windows a ETW a udalosťami zmeny registrov, napríklad vytvorením alebo úpravou kľúča slúžiaceho na perzistenciu. Pravidlá sú zámerne statické — nevyužívajú strojové učenie ani pravdepodobnostné skórovanie a každé má jednoznačne definovaný spúšťač, ktorý sa vyhodnotí ako pravdivý alebo nepravdivý. Vďaka tomu je každý zásah plne vysvetliteľný, auditovateľný a reprodukovateľný a analytik vždy presne vie, prečo pravidlo zareagovalo. Každý záznam databázy má päť stĺpcov: identifikátor techniky rámca MITRE ATT&CK, na ktorú je pravidlo namapované (napríklad T1113 Screen Capture alebo T1547 Boot or Logon Autostart Execution), typ telemetrie a spúšťacej udalosti, presnú spúšťaciu podmienku, krátky ľudsky čitateľný názov pravidla a podrobný popis detegovanej aktivity a jej kontextu. Mapovanie na rámec MITRE ATT&CK dáva pravidlám

spoločnú taxonómiu, umožňuje merať pokrytie útočnických techník, identifikovať medzery v detekcii, reportovať zistenia v jazyku zrozumiteľnom aj pre iné tímy a korelovať zistenia so správaním konkrétnych útočnických skupín. Súčasťou dokumentu sú aj ukážky čítania pravidiel a poznámky k údržbe a rozširovaniu katalógu.

Väzba na ciele projektu: Výstup naplňa špecifický cieľ 2 projektu — identifikáciu použiteľných metód dátovej analýzy a strojového učenia umožňujúcich automatizáciu analytickej práce forenzného analytika, konkrétne vyhľadávanie vzorcov správania v údajoch.

Zhodnotenie ukazovateľa: očakávaná hodnota dvoch publikovaných datasetov a databáz bola dosiahnutá v plnom rozsahu. Ukazovateľ je splnený. Obidva výstupy sú určené na verejné sprístupnenie v otvorených úložiskách v súlade so zásadami otvorenej vedy.

7 Publikované metodológie

Očakávaný počet	Reálne plnenie	Stav
3	3	Splnené

7.1 Vymedzenie ukazovateľa

Základom pre odhad bol počet metodológií, ktoré je potrebné pripraviť na dosiahnutie cieľov projektu. Na rozdiel od jednotlivých metód a modelov ide o ucelené metodické rámce, ktoré určujú, ako sa k danej úlohe pristupuje. Prvý rámec vymedzuje zmluvné a právne prostredie poskytovania služieb digitálnej forenzej analýzy, druhý určuje princípy a štádiá samotného spracovania digitálnych stôp a tretí postup tvorby časovej osi prípadu.

7.2 Prehľad výstupov

Číslo	Výstup	Pracovný balík	Zodpovedný partner	Prístup
D1	Metodológia pre zmluvné vzťahy	KPB1	EISI	Neverejný
D3	Metodológia postupu spracovania digitálnych stôp	KPB1	EISI	Verejný
D23	Metodológia pre tvorbu časovej osi prípadu	KPB5	UPJŠ	Verejný

7.3 D01 — Metodológia pre zmluvné vzťahy

Údaj	Hodnota
Číslo výstupu	D1
Pracovný balík / úloha	KPB1, úloha KPB1.1
Zodpovedný partner	European Information Society Institute
Typ	metodológia
Prístup a šírenie	neverejný — interný archív dokumentov projektu
Dokument s podrobným popisom	ADFIR-D1-KPB1-01-Metodika-zmluvnych-vztahov (SK)

Zhrnutie: Metodika vytvára jednotný rámec odporúčaní a postupov pre uzatváranie zmluvných vzťahov pri poskytovaní služieb digitálnej forenzej analýzy a reakcie na kybernetické incidenty. Jej cieľom je zabezpečiť právnu istotu, ochranu údajov, zachovanie dôkaznej hodnoty digitálnych dôkazov a efektívne riešenie bezpečnostných incidentov. Metodika systematizuje uzatváranie zmluvných vzťahov do dvoch nadväzujúcich fáz. V predzmluvnej fáze ide o identifikáciu potrieb a cieľov klienta, predbežnú analýzu jeho prostredia, overenie spôsobilosti poskytovateľa, ochranu dôverných informácií a posúdenie spracúvania osobných údajov. Vo fáze uzatvorenia zmluvy ide o voľbu vhodného zmluvného modelu, vymedzenie predmetu zmluvy a rozsahu oprávnení, úpravu dohody o úrovni služieb a reakčných časov, ochranu informácií a osobných údajov, nakladanie s digitálnymi dôkazmi, zodpovednosť za škodu, cenu, trvanie a ukončenie zmluvy, riešenie sporov a úpravu výstupov. Súčasťou dokumentu sú dve schémy zhrňajúce odporúčaný postup v oboch fázach. Metodika vychádza zo slovenského Obchodného zákonníka, z nariadenia o ochrane osobných údajov a z ďalších relevantných predpisov v oblasti kybernetickej bezpečnosti, ochrany obchodného tajomstva, autorského práva a trestného práva, a je ukotvená v technických normách radu ISO/IEC 27037, 27041, 27042 a 27043 a v norme ISO 21043-2. Argumentácia je doložená judikatúrou Najvyššieho správneho súdu SR a krajských súdov.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 3 projektu — využitie automatizácie digitálnej forenzej analýzy v trestnom konaní. Vytvára zmluvné a právne predpoklady pre to, aby výstupy automatizovanej forenzej analýzy obstáli pri posudzovaní ich prípustnosti a dôkaznej hodnoty.

7.4 D03 — Metodológia postupu spracovania digitálnych stôp

Údaj	Hodnota
Číslo výstupu	D3
Pracovný balík / úloha	KPB1, úloha KPB1.3
Zodpovedný partner	European Information Society Institute
Typ	metodológia
Prístup a šírenie	verejný — publikácia na webovom sídle projektu
Dokument s podrobným popisom	ADFIR-D3-KPB1-03-Metodologia-pre-spracovanie-digitalnych-stop (SK)
Dostupnosť	https://adfir.upjs.sk/

Zhrnutie: Metodológia vymedzuje princípy a štádiá spracovania digitálnych stôp tak, aby boli splnené požiadavky kladené na ich integritu, autenticitu, prípustnosť a relevantnosť. Dokument najprv vymedzuje základné východiská a následne formuluje päť princípov získavania, uchovávaní a interpretácie digitálnych dôkazov: identifikáciu nevyhnutného

a primeraného rozsahu skúmania, akvizíciu dostatočného množstva relevantných informácií, evidenciu a reťazenie dôkazov spolu s transparentnosťou, preskúmateľnosťou a hodnovernosťou postupu, nestrannosť a nezáujatosť a napokon rizikovú analýzu, taktiku a profesionalitu. Druhá časť metodológie rozpracúva päť štádií digitálnej analýzy — identifikáciu digitálnych informácií, zhromažďovanie dát, uchovávanie dát, overovanie dát a postupov a analýzu a interpretáciu dát. Metodológia tak poskytuje procesný rámec, ktorý prepája technickú realizáciu forenznnej analýzy s požiadavkami právneho poriadku a s technickými normami radu ISO/IEC 27037 až 27043.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 3 projektu. Metodológia je záväzným procesným rámcom pre všetky technické výstupy projektu, pretože určuje, za akých podmienok zostáva digitálna stopa spracovaná automatizovanými metódami použiteľná ako dôkaz.

7.5 D23 — Metodológia pre tvorbu časovej osi prípadu

Údaj	Hodnota
Číslo výstupu	D23
Pracovný balík / úloha	KPB5, úloha KPB5.1
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metodológia
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D23-KPB5-01-Metodologia-pre-tvorbu-casovej-osi-pripadu (SK)

Zhrnutie: Metodológia opisuje proces spracovania údajov pre časovú os prípadu a nástroj ETL Timeline, ktorý bol na tento účel vytvorený. Nástroj integruje výstupy dvoch nezávislých analytických tokov do jedného prostredia pre ich spoločnú interpretáciu: prepája štandardizované metazáznamy vytvorené z výstupov Eric Zimmerman’s nástrojov (EZ Tools) s analytickými výsledkami získanými nad údajmi spracovanými nástrojom Plaso. Udalosti získané z forenzných artefaktov sú tak zobrazené v spoločnom časovom kontexte spolu s výsledkami analýz, ako sú identifikované zhluky, anomálie, fázy útoku, či vzťahy medzi udalosťami. Dokument podrobne opisuje závislosti a prerekvizity nástroja, povinné aj voliteľné vstupné údaje, spôsob spustenia, spracovanie údajov na pozadí a vkladanie údajov. Osobitná časť je venovaná grafickému rozhraniu a jeho funkcionalitám — zobrazeniu grafu časovej osi, obohateniu časovej osi o výstupy ďalších analýz, práci s textovými údajmi a filtrovaní udalostí. Záverečná kapitola vymedzuje forenzný význam nástroja: integrovaný pohľad eliminuje potrebu manuálneho prepájania výsledkov z viacerých nástrojov a umožňuje analytikovi efektívnejšie identifikovať časové a logické súvislosti medzi jednotlivými udalosťami.

Väzba na ciele projektu: Výstup naplňa špecifický cieľ 2 projektu — automatizáciu analytickej práce forenzného analytika, konkrétne identifikáciu časového rámca bezpečnostného incidentu a jeho jednotlivých fáz.

Zhodnotenie ukazovateľa: očakávaná hodnota troch publikovaných metodológií bola dosiahnutá v plnom rozsahu. Ukazovateľ je splnený. Metodický rámec analýzy otvorených zdrojov ako dôkazu v trestnom konaní bol navyše publikovaný aj vo forme recenzovaného vedeckého článku (kapitola 3).

8 Publikované metódy a modely

Očakávaný počet	Reálne plnenie	Stav
10	12	Prekročené

8.1 Vymedzenie ukazovateľa

Základom pre odhad bol počet metód a modelov, ktoré je potrebné pripraviť na dosiahnutie cieľov projektu. Do ukazovateľa spadajú výstupy typu „metóda“ a „model“ naprieč pracovnými balíkmi KPB1 až KPB4. Všetky sú určené na zverejnenie, a to buď v otvorených repozitároch, alebo na webovom sídle projektu.

Výstupy D19 a D20 boli dodané ako dvojice samostatných výstupov, a to D19.1 a D19.2, resp. D20.1 a D20.2. Každý z nich rieši odlišný metodický prístup a je spracovaný ako samostatný dokument. Celkový počet publikovaných metód a modelov preto dosiahol dvanásť oproti desiatim plánovaným.

8.2 Prehľad výstupov

Číslo	Výstup	KPB	Typ	Zodp.
D02	Metóda na anonymizáciu digitálnych stôp	KPB1	metóda	EISI
D12	Metóda na automatizovaný zber digitálnych stôp	KPB2	metóda	IstroSec
D13	Metóda na tvorbu datasetu	KPB2	metóda	IstroSec
D15	Model na extrakciu digitálnych stôp do maticovej reprezentácie	KPB3	model	UPJŠ
D16	Model na extrakciu digitálnych stôp do grafovej reprezentácie	KPB3	model	UPJŠ
D17	Model na agregáciu a prepojenie digitálnych stôp	KPB3	model	UPJŠ
D18	Model na obohatenie digitálnych stôp	KPB3	model	IstroSec
D19.1	Metóda na identifikáciu digitálnych stôp — zhlukovanie a veľké jazykové modely	KPB4	metóda	UPJŠ
D19.2	Metóda na identifikáciu digitálnych stôp — detekcia anomálií	KPB4	metóda	UPJŠ

Číslo	Výstup	KPB	Typ	Zodp.
D20.1	Metóda na identifikáciu vzťahov — faktorizácia formálneho kontextu	KPB4	metóda	UPJŠ
D20.2	Metóda na identifikáciu vzťahov — významné časové okná	KPB4	metóda	UPJŠ
D21	Metóda na určenie časového rámca a fáz útoku	KPB4	metóda	UPJŠ

8.3 D02 — Metóda na anonymizáciu digitálnych stôp

Údaj	Hodnota
Číslo výstupu	D02
Pracovný balík / úloha	KPB1, úloha KPB1.2
Zodpovedný partner	European Information Society Institute
Typ	metóda
Prístup a šírenie	verejný — publikácia na webovom sídle projektu
Dokument s podrobným popisom	ADFIR-D2-KPB1-02-Metoda-pre-anonymizáciu-digitalnych-stop (SK)
Dostupnosť	https://adfir.upjs.sk/

Zhrnutie: Metóda vymedzuje postup anonymizácie digitálnych stôp tak, aby ich bolo možné využiť na výskumné účely a na tréningovanie modelov strojového učenia bez porušenia právneho rámca ochrany osobných údajov. Postup má štyri na seba nadväzujúce kroky. Prvým je inventarizácia a klasifikácia údajov, v rámci ktorej sa údaje triedia na osobné a neosobné a osobitne sa identifikujú iné druhy chránených informácií, napríklad obchodné tajomstvo. Druhým krokom je posúdenie súladu s právnymi požiadavkami na anonymizáciu osobných údajov, teda overenie, kedy anonymizovaný údaj prestáva byť osobným údajom v zmysle nariadenia o ochrane osobných údajov. Tretím krokom je výber anonymizačných metód, pričom metodika rozlišuje dve základné skupiny — randomizáciu a zovšeobecnenie — a uvádza podmienky ich vhodného použitia. Štvrtým krokom je kontrola výsledku, teda overenie, či anonymizovaný súbor neumožňuje spätnú identifikáciu dotknutých osôb. Záverečná časť sa venuje využitiu anonymizovaných digitálnych stôp pre budúcu analýzu, vrátane výkladu výnimky pre spracúvanie na účely vedeckého výskumu.

Väzba na ciele projektu: Výstup naplňa špecifický cieľ 3 projektu a zároveň je nevyhnutným predpokladom pre pracovné balíky KPB2 až KPB4, pretože umožňuje pracovať s digitálnymi stopami z reálnej praxe pri zachovaní ochrany osobných údajov.

8.4 D12 — Metóda na automatizovaný zber digitálnych stôp

Údaj	Hodnota
Číslo výstupu	D12
Pracovný balík / úloha	KPB2, úloha KPB2.1
Zodpovedný partner	IstroSec s. r. o.
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D12-KPB2-01-Metoda-na-automatizovany-zber-digitalnych-stop (SK)

Zhrnutie: Metóda definuje robustný a opakovateľný postup automatizovaného zberu forenzných artefaktov, ktorý zabezpečuje foreznú integritu a konzistenciu vytváraných dátových sád. Dokument systematicky mapuje hlavné kategórie forenzných artefaktov operačného systému Windows a ich zdroje a člení ich do skupín podľa výpovednej hodnoty: artefakty spúšťania programov a ich prítomnosti v systéme (Amcache, Background Activity Monitor, MUICache, Prefetch, RecentApps, RecentFileCache, RunMRU, Shimcache, System Resource Usage Monitor, UserAssist a Windows Activities), artefakty perzistencie (súbor DNS Hosts, perzistencia v registri, naplánované úlohy, služby, databázy Shim, súbory ovládačov a repozitár WMI) a artefakty používateľskej aktivity. Metóda počíta s hybridným prístupom, ktorý kombinuje zber údajov zo simulovaných útokov v kontrolovanom prostredí s anonymizovanými artefaktmi z reálnej praxe. Pre samotný zber a spracovanie navrhuje balík technologických riešení kombinujúci etablované priemyselné nástroje s internými nástrojmi spoločnosti IstroSec, pričom pre fázu rýchlej triáže a extrakcie štandardných artefaktov explicitne definuje využitie parserov forenzných artefaktov operačného systému Windows.

Väzba na ciele projektu: Výstup naplňuje špecifický cieľ 1 projektu — identifikáciu potenciálnych zdrojov forenzných artefaktov a ich zber pri zachovaní integrity a autenticity digitálnych stôp.

8.5 D13 — Metóda na tvorbu datasetu

Údaj	Hodnota
Číslo výstupu	D13
Pracovný balík / úloha	KPB2, úloha KPB2.2
Zodpovedný partner	IstroSec s. r. o.

Údaj	Hodnota
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D13-KPB2-02-Metoda-na-tvorbu-datasetu (SK)

Zhrnutie: Metóda rieši jednu z hlavných výziev oblasti, ktorou je nedostatok kvalitných forenzných dátových sád spĺňajúcich požiadavky na dostupnosť komplexných prípadových štúdií a na dostatočný počet relevantných digitálnych artefaktov. Dokument najprv rozlišuje tri základné typy dátových sád použiteľných pre strojové učenie v digitálnej forenznej analýze — reálne dátové sady získané priamo z riešenia skutočných bezpečnostných incidentov, sady vytvorené zo simulovaných útokov a techník útočníkov v kontrolovanom prostredí a databázy pochádzajúce zo súťaží Capture The Flag — a porovnáva ich výhody a obmedzenia. Následne predkladá dve nadväzujúce metódy. Prvá opisuje vytváranie forenzných dátových súborov na základe techník útočníkov a je demonštrovaná na scenári skupiny APT-19 s rozlíšením fázy prípravy a fázy vykonania útoku; osobitne sa venuje detekcii bezsúborových hrozieb a hrozieb založených na platforme .NET, zneužitíu dôveryhodných ciest a kamufláži a obchádzaniu moderných ochranných mechanizmov. Druhá metóda opisuje vytváranie forenzných dátových sád z materiálov súťaží Capture The Flag vrátane identifikácie možných zdrojov údajov.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu. Metóda je priamym predpokladom pre vznik datasetu D14 a zároveň umožňuje reprodukovateľné rozširovanie dátovej základne projektu o nové útočné scenáre.

8.6 D15 — Model na extrakciu digitálnych stôp do maticovej reprezentácie

Údaj	Hodnota
Číslo výstupu	D15
Pracovný balík / úloha	KPB3, úloha KPB3.1
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	model
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D15-KPB3-01-Model-na-extrakciu-digitalnych-stop-do-maticovej-reprezentacie (SK)

Zhrnutie: Model transformuje prevažne neštruktúrované a textové forenzné údaje do podoby vhodnej pre metódy strojového učenia a formálne analytické prístupy. Vstupným podkladom sú údaje získané nástrojom Plaso, ktorý agreguje a koreluje forenzné artefakty z rôznych zdrojov do jednotnej časovej osi, takzvanej supertimeline. Výsledná dátová štruktúra má charakter tabuľky pozostávajúcej zo 17 atribútov (okrem iného dátum, čas, časová zóna, časové pečiatky typu MACB, zdroj a typ zdroja). Model systematicky identifikuje relevantné atribúty a zakóduje ich do binárnych, kategorických alebo numerických premenných tak, aby sa minimalizovala strata informácie. Po zakódovaní vzniklo celkovo 769 atribútov. Vzhľadom na obmedzené výpočtové kapacity nebolo možné spracovať všetky atribúty naraz, preto bola metóda analýzy hlavných komponentov aplikovaná samostatne pre každý typ zdroja a následne boli jednotlivé dátové sady spojené do jednotnej reprezentácie. Výsledná maticová reprezentácia pozostáva zo 178 atribútov, ktoré tvoria jednotnú reprezentáciu údajov naprieč všetkými dátovými sadami; ku každému atribútu je uvedený zdrojový artefakt a slovný popis.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu — identifikáciu vhodnej reprezentácie forenzných artefaktov. Preklučuje medzeru medzi manuálnou forenznou analýzou a automatizovanými metódami spracovania údajov a tvorí základ pre nadväzujúcu agregáciu a prepojenie digitálnych stôp vo výstupe D17.

8.7 D16 — Model na extrakciu digitálnych stôp do grafovej reprezentácie

Údaj	Hodnota
Číslo výstupu	D16
Pracovný balík / úloha	KPB3, úloha KPB3.2
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	model
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D16-KPB3-02-Model-na-extrakciu-digitalnych-stop-do-grafovej-reprezentacie (SK)

Zhrnutie: Model predstavuje prostriedok na systematickú transformáciu forenzných artefaktov z nesúrodých dátových zdrojov do jednotnej grafovej štruktúry. Digitálne stopy sú reprezentované ako množina uzlov a hrán, kde uzly predstavujú napríklad zariadenia, používatel'ov, procesy, súbory alebo komunikačné entity a hrany vyjadrujú ich vzájomné väzby, interakcie alebo kauzálne nadväznosti. Na rozdiel od tabuľkovej reprezentácie umožňuje grafový model zachytiť nielen samotné objekty forenznej analýzy, ale aj ich kontext a časové súvislosti, čo je v prostredí digitálnej forenznej analýzy jedným z kľúčových predpokladov úspešnej rekonštrukcie udalostí. Súčasťou výstupu sú grafové procesné a stavové diagramy, ktoré poskytujú základ pre následnú analýzu priebehu incidentu,

identifikáciu kľúčových udalostí a odhalenie anomálnych štruktúr v údajoch. Model je teoreticky ukotvený v teórii grafov, v konceptuálnom modelovaní informačných systémov a v riadení podnikových procesov. Dokument zároveň naznačuje ďalšie smerovanie — pomocou grafových algoritmov, napríklad hľadania podgrafov, je možné identifikovať vzory reprezentujúce typické známe schémy útokov a buď predikovať ich vývoj v reálnom čase, alebo v rámci analýzy po incidente získať nové informácie o správaní útočníka.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu a zároveň vytvára predpoklad pre špecifický cieľ 2, pretože grafová reprezentácia je vstupom pre metódu identifikácie vzťahov medzi digitálnymi stopami vo výstupe D20.

8.8 D17 — Model na agregáciu a prepojenie digitálnych stôp

Údaj	Hodnota
Číslo výstupu	D17
Pracovný balík / úloha	KPB3, úloha KPB3.3
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	model
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D17-KPB3-03-Model-na-agregáciu-a-prepojenie-digitalnych-stop (SK)

Zhrnutie: Model umožňuje systematické spracovanie forenzných artefaktov, redukciu množstva záznamov, ich koreláciu naprieč rôznymi zdrojmi a interpretáciu v kontexte identifikovaných scenárov správania systému alebo používateľa. Kľúčovým pojmom modelu je metazáznam — logicky ucelená jednotka informácie, ktorá vzniká spojením viacerých forenzných stôp na základe časovej, identitnej alebo kontextovej väzby. Proces definovania metazáznamov pozostával z identifikácie relevantných scenárov správania, ako sú autentifikácia, vzdialený prístup, manipulácia so súbormi alebo perzistencia, ku ktorým boli následne priradené forenzné artefakty schopné indikovať výskyt danej udalosti. Metazáznamy sa následne agregujú do väčších analytických celkov s cieľom znížiť fragmentáciu evidovaných udalostí a vytvoriť prehľadnejší obraz o priebehu analyzovaných aktivít; prvým spôsobom agregácie je zoskupovanie podľa zvoleného časového okna, ktorého veľkosť je možné prispôbiť charakteru analyzovaných údajov, čím vznikajú časové úseky reprezentujúce napríklad reláciu používateľa, fázu útoku alebo samostatný incident. Osobitná kapitola rieši agregáčnne funkcie vzhľadom na neznáme hodnoty a rozlišuje tri sémantické prípady — keď sú hodnoty 0 a 1 rovnako významné, keď je hodnota 1 významnejšia ako 0 a keď sú hodnoty 0 a neznáma hodnota rovnako významné. Všetky tri prípady sú zapísané jednou zovšeobecnenou váženou funkciou s koeficientmi, ktoré sa volia podľa sémantiky problému,

čo umožňuje implementovať jedinú modulárnu funkciu meniacu správanie len nastavením váh. Model pracuje s výstupmi nástrojov Erica Zimmermana (EvtxECmd, MFTECmd, RECmd) a obsahuje aj návrh vizualizácie agregovaných digitálnych stôp.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu. Nadväzuje na maticovú reprezentáciu z výstupu D15 a umožňuje vyššiu úroveň abstrakcie, korelácie a interpretácie udalostí.

8.9 D18 — Model na obohatenie digitálnych stôp

Údaj	Hodnota
Číslo výstupu	D18
Pracovný balík / úloha	KPB3, úloha KPB3.4
Zodpovedný partner	IstroSec s. r. o.
Typ	model
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D18-KPB3-04-Model-na-obohatenie-digitalnych-stop (SK)

Zhrnutie: Model vytvára ucelený rámec systematického dopĺňania kontextu k digitálnym stopám prepájaním artefaktov s externými zdrojmi, indikátormi kompromitácie a spravodajskými informáciami o hrozbách. Dokument najprv vymedzuje možnosti digitálneho obohacovania dôkazov a zložitost' obohacovania artefaktu vo fáze predspracovania, následne systematicky spracúva jednotlivé typy obohaciteľných údajov. Pre každý typ uvádza jednotnú trojicu informácií — význam a použitie, typické artefakty, ktoré daný údaj obsahujú, a spôsoby a nástroje na jeho obohatenie. Katalóg pokrýva okrem iného kľúče a tokeny rozhraní API, identifikátory cloudových zdrojov, podpisy kódu, adresy kryptomenových peňaženiek, identifikátory zraniteľností CVE, digitálne certifikáty, dopyty DNS, e-mailové adresy, kryptografické odtlačky súborov a plne kvalifikované doménové mená. Výsledkom je flexibilný a škálovateľný model podporujúci rôzne úrovne obohacovania, od jednoduchých atribútov až po komplexné zložené informácie. Model umožňuje presnejšie vyhodnocovanie a riešenie incidentov, rýchlejšiu atribúciu útoku a lepšiu prioritizáciu činností počas reakcie na incident aj počas forenznej analýzy.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 1 projektu a zvyšuje výpovednú hodnotu digitálnych stôp pre analytické metódy pracovného balíka KPB4.

8.10 D19.1 — Metóda na identifikáciu digitálnych stôp: zhlukovanie a veľké jazykové modely

Údaj	Hodnota
Číslo výstupu	D19.1
Pracovný balík / úloha	KPB4, úloha KPB4.1
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D19-KPB4-01-01-Metoda-na-identifikáciu-digitalnych-stop (SK)

Zhrnutie: Výstup skúma dva odlišné prístupy k identifikácii digitálnych stôp — zhlukovaciú analýzu a veľké jazykové modely. V časti venovanej zhlukovaniu zavádza forenzné metriky zhlukov, validačné metriky na určenie počtu zhlukov a postup hľadania anomálií zhlukovaním, ktoré následne aplikuje hierarchickým zhlukovaním na predspracované dátové súbory s dôrazom na vysvetliteľnosť výsledkov. V časti venovanej veľkým jazykovým modelom opisuje predspracovanie údajov, samotnú analýzu, vyhodnotenie úspešnosti a interpretovateľnosť výsledkov. Záver konštatuje, že zámerom nebolo vytvoriť univerzálny automatizovaný systém nahrádzajúci prácu analytika, ale overiť, do akej miery môžu vybrané metódy podporiť analýzu rozsiahlych a komplexných dátových množín, v ktorých je manuálne vyhľadávanie relevantných udalostí časovo náročné a prakticky obmedzené. Hierarchické zhlukovanie sa ukázalo ako vhodný nástroj pre dátové množiny, v ktorých nie je možné vopred definovať počet ani charakter jednotlivých skupín, čo je významné najmä pri práci s neznámymi aktivitami; veľké jazykové modely naproti tomu prinášajú schopnosť interpretovať komplexné textové reprezentácie a poskytnúť kontextové vysvetlenie identifikovaných udalostí. Čiastkové výsledky boli publikované v recenzovanej vedeckej práci o identifikácii relevantných forenzných artefaktov pomocou agregácie do časových okien a hierarchického zhlukovania, ktorá zaviedla metriky attack rate a attack lift.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 2 projektu — identifikáciu použiteľných metód dátovej analýzy a strojového učenia umožňujúcich automatizáciu analytickej práce forenzného analytika.

8.11 D19.2 — Metóda na identifikáciu digitálnych stôp: detekcia anomálií

Údaj	Hodnota
Číslo výstupu	D19.2

Údaj	Hodnota
Pracovný balík / úloha	KPB4, úloha KPB4.1
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D19-KPB4-01-02-Metoda-na-identifikáciu-digitalnych-stop (SK)

Zhrnutie: Výstup rieši identifikáciu digitálnych stôp detekciou anomálií metódami učenia bez učiteľa. Teoretická časť vymedzuje detekciu anomálií, jej realizáciu bez učiteľa a tri typy anomálií — bodové, kontextové a kolektívne — a kategorizuje dostupné metódy detekcie. Aplikačná časť opisuje použité dátové súbory a ich spracovanie a experimentálne porovnáva osem metód: analýzu hlavných komponentov, Local Outlier Factor, Subspace Outlier Detection, Empirical-Cumulative-distribution-based Outlier Detection, Copula-Based Outlier Detection, Isolation Forest, Isolation-based Nearest Neighbour Ensemble a Lightweight On-line Detector of Anomalies. Porovnanie prebieha v troch rovinách — nastavenie experimentov, vyhodnotenie úspešnosti detekcie a porovnanie výpočtovej náročnosti — a je doplnené o interpretáciu výsledkov. Čiastkové výsledky boli publikované v dvoch recenzovaných vedeckých prácach projektu: v štúdiu o detekcii anomálií v prehliadači Mozilla Firefox, ktorá identifikovala metódy ECOD a COPOD ako najvhodnejší kompromis medzi presnosťou a objemom výstupných údajov, a v štúdiu o vplyve antiforenzných techník na presnosť algoritmickej detekcie anomálií.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 2 projektu. Detekcia anomálií predstavuje kľúčový prístup k identifikácii relevantných digitálnych stôp v prostredí, v ktorom nie sú k dispozícii anotované údaje.

8.12 D20.1 — Metóda na identifikáciu vzťahov: faktorizácia formálneho kontextu

Údaj	Hodnota
Číslo výstupu	D20.1
Pracovný balík / úloha	KPB4, úloha KPB4.2
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch

Údaj	Hodnota
Dokument s podrobným popisom	ADFIR-D20-KPB4-01-Metoda-na-identifikáciu-vztahov (SK)

Zhrnutie: Výstup rieši identifikáciu vzťahov v údajoch z digitálnej forenzej analýzy maticovou faktorizáciou založenou na formálnych konceptoch. Po vymedzení formálnej konceptovej analýzy dokument postupne rozpracúva dekompozíciu formálneho kontextu — faktorizáciu binárnych matíc, chápanie formálnych konceptov ako faktorov a problém pokrytia množiny — a predstavuje algoritmus RSF, ktorý kombinuje hladový výber s postupným vytváraním kandidátnych formálnych konceptov. Výsledkom je presný rozklad vstupnej incidenčnej matice, ktorý umožňuje identifikovať skupiny objektov charakterizované spoločnými atribútmi a zachytiť vzťahy medzi časovými zhukmi udalostí a ich vlastnosťami. Faktory s menším počtom atribútov spravidla opisujú všeobecnejšie vzory prítomné pri väčšom počte objektov, zatiaľ čo faktory s väčším počtom atribútov zachytávajú špecifickejšie kombinácie vlastností a ich extenty sú menšie. Aplikačná časť rozlišuje všeobecné a špecifické faktory a osobitne faktory súvisiace s útokom a ukazuje, že pri analýze je možné zamerať sa na vybraný významný atribút a sledovať, s ktorými ďalšími atribútmi sa v jednotlivých faktoroch vyskytuje. Dôležitým prínosom metódy je interpretovateľnosť nájdených faktorov.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 2 projektu, konkrétne identifikáciu vzťahov medzi digitálnymi stopami ako jednu zo štyroch oblastí dôležitých pre prácu forenzného analytika.

8.13 D20.2 — Metóda na identifikáciu vzťahov: významné časové okná

Údaj	Hodnota
Číslo výstupu	D20.2
Pracovný balík / úloha	KPB4, úloha KPB4.2
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D20-KPB4-02-Metoda-na-identifikáciu-vztahov (SK)

Zhrnutie: Výstup rozpracúva metódu na identifikáciu významných časových okien vo forenzných údajoch, ktoré môžu poukazovať na výskyt neštandardnej alebo bezpečnostne relevantnej aktivity. Metóda vychádza z formálnej konceptovej analýzy a z atribútových implikácií a využíva opakujúce sa kombinácie atribútov špecifické pre vybrané časti dátovej

sady. Výstupom sú časové pravidlá prepájajúce uzavretý atribútový opis skupiny objektov s konkrétnym časovým oknom, takže metóda okrem lokalizácie časového úseku poskytuje aj jeho charakteristiky využiteľné pri ďalšej forenznej analýze. Metóda zámerne negeneruje všetky platné atribútové implikácie s časovým atribútom v konzekvente, ale pre každý identifikovaný časovo homogénny extant vytvára iba jedno pravidlo s maximálnym antecedentom, čím redukuje redundanciu výsledných pravidiel. Výstup závisí od parametra k_{max} , ktorý predstavuje kompromis medzi rozsahom prehľadávania a výpočtovou náročnosťou: vyššie hodnoty môžu viesť k identifikácii ďalších časovo špecifických extantov, počet preverovaných kandidátnych množín však s rastúcim počtom atribútov prudko narastá. V použitej dátovej sade postačovala na identifikáciu významných časových okien už hodnota k_{max} rovná trom. Čiastkové výsledky formálnej konceptovej analýzy nad foreznými údajmi boli publikované v recenzovanej vedeckej práci venovanej atribútovým závislostiam dátovej sady NIST Data Leakage Case, v ktorej bol nad dátovou sadou s 10 306 záznamami a 11 binárnymi atribútmi skonštruovaný konceptuálny zväz s 26 formálnymi konceptmi.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 2 projektu a zároveň priamo podporuje určenie časového rámca incidentu riešené vo výstupe D21.

8.14 D21 — Metóda na určenie časového rámca a fáz útoku

Údaj	Hodnota
Číslo výstupu	D21
Pracovný balík / úloha	KPB4, úloha KPB4.3
Zodpovedný partner	Univerzita Pavla Jozefa Šafárika v Košiciach
Typ	metóda
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D21-KPB4-03-Metoda-na-urcenie-casoveho-ramca-a-faz-utoku (SK)

Zhrnutie: Metóda rekonštruje a analyzuje digitálne stopy prostredníctvom analýzy časových radov s cieľom posunúť foreznú analýzu od manuálneho prehliadania protokolov k poloautomatizovanému určeniu časového rámca začiatku útoku a jeho jednotlivých fáz. Časové rady boli vytvorené z relevantných artefaktov viacerých typov — protokolov udalostí Windows, hlavnej tabuľky súborov, monitora využitia systémových zdrojov a registrov — nad štyrmi simulovanými incidentmi. Metóda sleduje tri ciele: určenie okamihu prvej anomálnej aktivity, vytvorenie vstupnej vrstvy pre automatizovanú detekciu anomálií metódami strojového učenia a vygenerovanie zredukovanej časovej osi útoku prepájajúcej súvisiace udalosti z rôznych zdrojov.

Väzba na ciele projektu: Výstup naplňa špecifický cieľ 2 projektu — identifikáciu časového rámca bezpečnostného incidentu alebo trestného činu, prípadne čiastkových časových úsekov jednotlivých akcií, ako jednej zo štyroch oblastí dôležitých pre prácu forenzného analytika.

Zhodnotenie ukazovateľa: očakávaná hodnota desiatich publikovaných metód a modelov bola dosiahnutá v plnom rozsahu. Ukazovateľ je splnený. Čiastkové výsledky metód z pracovného balíka KPB4 boli publikované aj vo forme recenzovaných vedeckých prác na medzinárodných konferenciách ARES 2025, ITAT 2025 a CISIS 2026 (kapitola 3). Výstupy určené na zverejnenie budú sprístupnené v otvorených repozitároch, resp. na webovom sídle projektu v súlade so zásadou otvoreného prístupu deklarovanou v opise projektu.

9 Ďalšie zverejnené výstupy projektu

Nad rámec výstupov spadajúcich pod merateľné ukazovatele uvedené v kapitolách 6 až 8 vznikol v projekte ďalší verejný výstup typu „správa“, ktorý je svojím charakterom aplikačným zhrnutím výsledkov celého projektu a preto sa uvádza v samostatnej kapitole.

9.1 D24 — Rozšírená správa z forenznnej analýzy

Údaj	Hodnota
Číslo výstupu	D24
Pracovný balík / úloha	KPB5, úloha KPB5.2
Zodpovedný partner	IstroSec s. r. o.
Typ	správa
Prístup a šírenie	verejný — publikácia v otvorených repozitároch
Dokument s podrobným popisom	ADFIR-D24-KPB5-02-Rozsireny-report-z-forenznej-analyzy (SK)

Zhrnutie: Výstup predstavuje vzorovú štruktúru rozšírenej správy z forenznnej analýzy, ktorá integruje výsledky metód a modelov vytvorených v pracovných balíkoch KPB2 až KPB4 do podoby použiteľnej v praxi bezpečnostných tímov aj pri právnom posudzovaní. Správa sa otvára manažérskym zhrnutím a metodológiou, v ktorej sa uvádzajú zdroje dôkazov, spôsoby ich spracovania a parsovania a prístup k obohacovaniu. Nasledujú informácie o vyšetřovaných dôkazoch vrátane typu dôkazu a kryptografických odtlačkov a informácie o skúmanom zariadení — názov, verzia operačného systému, posledný čas vypnutia, adresa IP a sieťové nastavenia, nainštalované programy a použiteľné obohatenia. Jadrom dokumentu sú zistenia členené podľa forenzných kategórií: artefakty spúšťania programov (Prefetch, Amcache, monitor využitia systémových zdrojov, Background a Desktop Activity Moderator, UserAssist, Shimcache, RecentFileCache, RunMRU a ďalšie), artefakty perzistencie (kľúče Run a RunOnce, naplánované úlohy, služby, priečinky po spustení, perzistencia cez WMI a perzistencia v registri), analýza protokolov (záznamy vzdialeného prístupu, Sysmon, PowerShell, plánovač úloh, aplikačné protokoly, firewall, DNS, proxy, VPN a upozornenia z nástrojov EDR, SIEM a antimalvérových riešení) a artefakty používateľskej aktivity (história prehliadača a sťahovania, RecentDocs, naposledy použité dokumenty a dôveryhodné dokumenty balíka Office). Každá kategória je uzavretá voliteľným zhrnutím, čo umožňuje správu použiť ako šablónu aj pri čiastkových analýzach.

Väzba na ciele projektu: Výstup napĺňa špecifický cieľ 2 projektu a zároveň špecifický cieľ 4 — šírenie výsledkov projektu odbornej verejnosti, najmä bezpečnostným expertom a tímom. Správa prepája analytické výstupy projektu do formátu, ktorý je zrozumiteľný pre zadávateľa analýzy aj pre orgány činné v trestnom konaní.