Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

IADITPAI

Integrovaná a agregovaná dátová IT platforma využívajúca umelú inteligenciu

Odborný white paper: dátová integrácia, kontextová AI/RAG, automatizácia expertného know-how a validačný rámec

Prijímateľ	**TYRON COMPANY, s. r. o.**
Názov projektu	**Integrovaná a agregovaná dátová IT platforma využívajúca AI**
Kód projektu	**17I04-04-V05-00017**
Typ aktivity	Experimentálny vývoj; technologická pripravenosť TRL 3 → TRL 8
Obdobie realizácie	20. 06. 2026 – 14. 08. 2026
Miesto realizácie	Štefánikova 2/3, 949 01 Nitra, Nitriansky kraj
Doména RIS3	3-2 Zvýšenie úžitkovej hodnoty všetkých druhov údajov a databáz
Vydanie	1.0 | verejná odborná publikácia | august 2026

TYRON COMPANY, s. r. o. • Cabaj – Čápor • 2026

O publikácii a úroveň dôkazov

Táto publikácia je odborným výstupom výskumno-vývojového projektu IADITPAI. Vysvetľuje výskumné východiská, referenčnú architektúru, dátový a AI životný cyklus, bezpečnostný model a spôsob validácie integrovanej dátovej platformy. Text je koncipovaný ako samostatný white paper: spája projektové zadanie s overiteľnými návrhovými rozhodnutiami, experimentmi a metrikami, nie ako marketingový opis produktu.

Publikácia napĺňa vedľajší merateľný ukazovateľ „Počet odborných publikácií vytvorených v rámci projektu“ s východiskovou hodnotou 0 a plánovanou hodnotou 1. Zároveň podporuje diseminácia výsledkov projektu a zrozumiteľný prenos poznatkov medzi vývojovým tímom, prevádzkovými odborníkmi, manažmentom a pilotnými používateľmi.

Úroveň tvrdení Architektonické a metodické závery vychádzajú z projektovej dokumentácie a z odborných rámcov uvedených v kapitole 18. Cieľové KPI sú validačné hypotézy projektu.

Verejná verzia zámerne neobsahuje produkčné adresy, prihlasovacie údaje, zdrojový kód, citlivé dátové schémy, detailné konfigurácie zákazníkov ani tréningové dáta. Nenahrádza technickú dokumentáciu, bezpečnostné testy, akceptačné protokoly ani záznamy o riadení modelov.

Bibliografické a používateľské údaje

Položka	Údaj
Vydavateľ	TYRON COMPANY, s. r. o., Čápor 1098, 951 17 Cabaj – Čápor
Miesto a rok	Cabaj – Čápor, 2026
Forma	Elektronická odborná publikácia / white paper
Cieľové skupiny	IT prevádzka a bezpečnosť, dátoví a integrační architekti, AI/ML špecialisti, MSP, verejný sektor, manažment
Odporúčaná citácia	TYRON COMPANY, s. r. o. (2026). IADITPAI: Integrovaná a agregovaná dátová IT platforma využívajúca umelú inteligenciu. Odborný white paper. Projekt 17I04-04-V05-00017.

Executive summary

Organizácie prevádzkujú súbežne monitoring infraštruktúry, bezpečnostné sondy, cloudové služby, IoT zariadenia a ITSM nástroje. Každá vertikála vytvára vlastný tok udalostí, metrík a upozornení. Bez spoločného kontextu sa rovnaký incident javí ako niekoľko nesúvisiacich problémov, vzniká alert fatigue a rozhodovanie zostáva závislé od malého počtu seniorných špecialistov.

IADITPAI navrhuje horizontálnu, vendor-agnostic nadstavbu nad existujúcim technologickým prostredím. Konektorová vrstva zbiera údaje cez API, databázové a súborové rozhrania; integračná vrstva ich validuje, normalizuje do kanonického modelu a obohacuje o časový, topologický a prevádzkový kontext. Nad tým pracuje AI analytická vrstva kombinujúca strojové učenie, detekciu anomálií, RAG a pravidlá odvodené z expertného know-how.

Výstupom AI nie je autonómne rozhodnutie bez kontroly, ale prioritizované, zdrojmi podložené odporúčanie s mierou dôvery, vysvetlením a možnosťou schválenia človekom. Operátor dostáva takmer reálny pohľad v Grafane; manažment dlhodobé trendy, controlling a reportovanie v Power BI. Predvolená prevádzka on-prem podporuje dátovú suverenitu, pričom PaaS zostáva voliteľným modelom pre vhodné scenáre.

Projekt má charakter experimentálneho vývoja. Vychádza z TRL 3, vytvára integrovaný prototyp, overuje ho v relevantnom a následne reálnom prostredí a smeruje k TRL 8. Cieľovými validačnými hypotézami sú skrátenie MTTD/MTTR o 30–50 %, zníženie nákladov na špecialistov o 20–30 %, obmedzenie nerelevantných alertov o 40 %, zvýšenie využitia existujúcich technológií nad 70 % a zrýchlenie onboardingu nových technológií o 25–35 %.

Abstrakt

Publikácia predstavuje referenčný návrh integrovanej a agregovanej dátovej IT platformy využívajúcej umelú inteligenciu. Jadrom riešenia je oddelenie zdrojových technológií od kanonického dátového modelu, kontextová korelácia udalostí a riadené využitie RAG a strojového učenia na tvorbu odporúčaní pre IT prevádzku a bezpečnosť. Práca definuje návrhové invarianty, hranice dôvery, dátový a modelový životný cyklus, human-in-the-loop kontrolu, hrozby a validačný rámec pre prechod z TRL 3 na TRL 8.

Kľúčové slová: dátová integrácia; agregácia; umelá inteligencia; RAG; detekcia anomálií; IT operations; kybernetická bezpečnosť; explainability; human-in-the-loop; TRL.

Abstract

This paper presents a reference design for an integrated and aggregated AI-enabled IT data platform. The solution decouples source technologies from a canonical event model, correlates heterogeneous operational and security signals, and combines retrieval-augmented generation, machine learning and codified expert knowledge to produce traceable recommendations. The paper defines architectural invariants, trust boundaries, data and model lifecycles, human oversight, threat scenarios and a validation framework for progressing from TRL 3 to TRL 8.

Keywords: data integration; aggregation; artificial intelligence; RAG; anomaly detection; IT operations; cybersecurity; explainability; human-in-the-loop; technology readiness level.

1. Výskumný problém, ciele a metodika

1.1 Fragmentácia prevádzkových a bezpečnostných dát

Výskumný problém vzniká na rozhraní heterogénnosti dát, nejednotnej sémantiky a nedostatku expertných kapacít. Monitoring, SIEM/SOAR, APM, cloudové platformy a ITSM poskytujú kvalitné lokálne signály, ale typicky optimalizujú jednu doménu. Chýba spoločná vrstva, ktorá by udalosti zaradila do topológie služieb, zohľadnila závislosti aktív, históriu incidentov, prevádzkové zmeny a organizačné priority.

Dôsledkom je vysoký objem duplicitných upozornení, ručné prepájanie údajov a oneskorené rozhodnutie. Platforma preto nemá nahradiť zdrojové nástroje. Jej výskumným prínosom je zistiť, za akých podmienok možno nad nimi vybudovať horizontálnu kontextovú a rozhodovaciu vrstvu bez straty pôvodu dát a bez povinného presunu surových logov mimo prostredia organizácie.

1.2 Výskumné otázky

ID	Výskumná otázka	Overiteľný artefakt
RQ1	Ako zjednotiť udalosti z rozdielnych nástrojov bez pevnej väzby na konkrétneho výrobcu?	Konektory, kanonická schéma, mapovacie pravidlá a testy kompatibility
RQ2	Ako korelovať prevádzkové a bezpečnostné signály tak, aby sa znížil šum bez potlačenia kritických udalostí?	Korelačný model, zlatá validačná množina, precision/recall a miera redukcie alertov
RQ3	Ako využiť RAG a generatívny model tak, aby odporúčanie bolo zdrojované, kontrolovateľné a bezpečné?	Znalostná báza, evidencia citácií, confidence, guardrails a human-in-the-loop
RQ4	Ako kodifikovať seniorné know-how bez vytvorenia netransparentnej automatizácie?	Pravidlá, rozhodovacie stromy, playbooky, vlastníctvo a verzovanie znalostí
RQ5	Ako preukázať technologickú pripravenosť riešenia na úrovni TRL 8?	Protokoly modulových, integračných, bezpečnostných, výkonnostných a pilotných skúšok

1.3 Metodický rámec

Fáza	Metóda	Výstup / rozhodovacie kritérium
Poznanie problému	Rozhovory, pozorovanie práce, analýza zdrojových systémov a incidentov	Katalóg používateľov, use-case, dátových zdrojov a obmedzení
Návrh	Systémové inžinierstvo, SysML/UML, dátové modelovanie, threat modelling	Architektúra, rozhrania, dátové toky, hranice dôvery
Implementácia	Iteratívny experimentálny vývoj, Agile, DevSecOps, CI/CD	Integrovaný prototyp a reprodukovateľné zostavenie

Fáza	Metóda	Výstup / rozhodovacie kritérium
Verifikácia	Unit, contract, integračné, bezpečnostné, výkonnostné a UX testy	Dôkaz, že artefakt spĺňa špecifikované požiadavky
Validácia	Pilotné scenáre, A/B porovnanie, baseline vs. cieľ, spätná väzba	Dôkaz užitočnosti a pripravenosti v reálnom prostredí
Učenie	Post-incident review, analýza odchýlok, revízia pravidiel/modelov	Aktualizovaný know-how balík a register rizík

2. Architektonické požiadavky a návrhové invarianty

Návrhový invariant je vlastnosť, ktorá musí zostať pravdivá pri každej implementačnej variante. Invarianty oddeľujú podstatu výskumného riešenia od konkrétneho technologického zásobníka a umožňujú testovať, či integrácia, AI a prevádzka zachovali zamýšľané bezpečnostné a kvalitatívne vlastnosti.

Invariant	Požiadavka	Spôsob overenia
Vendor neutrality	Jadro platformy nesmie závisieť od proprietárnej schémy jedného zdroja.	Contract test konektora, mapovanie do kanonického modelu
Proveniencia	Každý odvodený signál musí byť spätne priraditeľný k zdroju, času a transformáciám.	Trace ID, lineage záznam, auditná stopa
Dátová suverenita	Citlivé surové dáta zostávajú predvolene v prostredí zákazníka.	Kontrola dátových tokov, egress test, konfiguračný audit
Oddelenie faktu a inferencie	Zistenie zo zdroja, pravidlový záver a generovaný návrh musia byť rozlíšiteľné.	Typovanie výstupu, citácie a označenie confidence
Ľudská kontrola	Riziková akcia nesmie byť vykonaná iba na základe nekontrolovaného generovaného textu.	Schvaľovací krok, politika oprávnení, rollback
Fail-safe prevádzka	Výpadok AI nesmie prerušiť základný zber, ukladanie a dostupnosť surových udalostí.	Degradačný test, queueing, replay a recovery
Pozorovateľnosť	Každá vrstva poskytuje metriky, logy, trace a stav kvality.	SLO dashboard, syntetické testy, alerty
Verzovateľnosť	Schémy, konektory, pravidlá, znalosti a modely majú identifikovateľnú verziu.	Registry artefaktov, SBOM/MBOM, release evidence

Kľúčový invariant IADITPAI môže odporučiť, prioritizovať a vysvetliť; zmenu v produkčnom prostredí vykoná iba autorizovaný workflow s explicitnou politikou a auditnou stopou.

3. Konektorová a dátová integračná vrstva

3.1 API-first integrácia a kontrakty

Konektor je adaptačná hranica medzi zdrojovým systémom a kanonickým modelom. Jeho úlohou nie je iba prenos správ, ale aj autentizácia, limitovanie požiadaviek, zachytenie zmeny schémy, normalizácia času, deduplikácia a priradenie pôvodu. API-first neznamená výlučne REST; zahŕňa aj streaming, databázové čítanie, webhook, správové fronty a kontrolovaný súborový import.

Krok	Kontrola	Výsledok pri chybe
Príjem	Identita zdroja, podpis/token, čas, povolený formát	Odmietnutie alebo karanténa
Syntaktická validácia	Schéma, povinné polia, typy, veľkosť	Dead-letter queue a metrika kvality
Sémantické mapovanie	Aktívum, služba, závažnosť, kategória, jednotky	Označenie neúplnosti; bez tichej aproximácie
Normalizácia	UTC čas, identifikátory, taxonómia, deduplikácia	Deterministický replay pôvodnej udalosti
Obohatenie	Topológia, vlastník, kritickosť, zmena, hrozba	Oddelenie chýbajúceho kontextu od chyby zdroja
Publikovanie	Idempotencia, poradie, retenčná trieda, trace ID	Retry s limitom; ochrana pred duplikáciami

3.2 Kanonický model udalosti

Minimálny kanonický záznam obsahuje identitu zdroja a udalosti, čas vzniku a prijatia, typ objektu, dotknuté aktívum alebo službu, závažnosť, pozorované hodnoty, stav kvality, referenciu na pôvodný záznam a trace ID. Kontextové polia sa dopĺňajú ako samostatné atribúty s uvedením zdroja, aby obohatenie neprepisovalo originál.

Pravidlo kvality Normalizácia nesmie odstrániť pôvodný význam. Ak mapovanie nie je jednoznačné, systém uchová pôvodnú hodnotu a explicitne označí neistotu.

4. AI analytická vrstva: korelácia, ML a RAG

4.1 Rozdelenie zodpovedností

AI vrstva je navrhnutá ako súbor spolupracujúcich, ale oddeliteľne testovateľných funkcií. Deterministické pravidlá riešia známe podmienky a bezpečnostné obmedzenia. Štatistické a ML modely hľadajú anomálie a vzory. RAG vyberá relevantné znalosti a poskytuje ich generatívnemu modelu, ktorý zostaví zrozumiteľné odporúčanie. Orchestrátor uplatní politiku, označí dôveru a odošle výsledok človeku alebo povolenému workflow.

Komponent	Vstup	Výstup	Hlavná kontrola
Korelácia	Normalizované udalosti, topológia a časové okná	Skupina súvisiacich udalostí / incidentný kandidát	Deterministické pravidlá a spätná reprodukcia
Detekcia anomálií	Časové rady, baseline, sezónnosť	Skóre odchýlky a relevantné črty	Drift, false positive rate, citlivosť
Retriever	Otázka, incidentný kontext, oprávnenia	Zoradené znalostné fragmenty	ACL filter, aktuálnosť, relevance@k
Generátor	Fakty, fragmenty, šablóna a obmedzenia	Vysvetlenie a návrh krokov	Citácie, groundedness, zakázané akcie
Policy/orchestrátor	Návrh, rola, kritickosť, confidence	Zobraziť, eskalovať, vyžiadať schválenie	Policy-as-code a audit rozhodnutia

4.2 RAG pipeline a dôveryhodnosť

1. Zostaviť dotaz iba z povoleného incidentného kontextu a odfiltrovať tajomstvá alebo osobné údaje, ktoré nie sú potrebné.
2. Vyhľadať znalostné fragmenty v rozsahu oprávnení používateľa a zachovať identitu dokumentu, verziu a dátum účinnosti.
3. Preusporiadať kandidátov podľa relevancie, aktuálnosti, dôveryhodnosti zdroja a kompatibility s dotknutou technológiou.
4. Vytvoriť odpoveď v štruktúre: pozorované fakty, hypotéza príčiny, odporúčané kroky, riziká, predpoklady a citované zdroje.
5. Validovať formát, zakázané príkazy, minimálnu oporu v zdrojoch a prah dôvery; pri nesplnení odpoveď označiť alebo zablokovať.
6. Zaznamenať vstupný kontext, identifikátory zdrojov, verziu modelu, konfiguráciu a rozhodnutie používateľa pre audit a učenie.

4.3 Hodnotenie odporúčaní

Dimenzia	Metrika / test	Akceptačný princíp
Relevantnosť	Precision@k, nDCG, hodnotenie expertom	Použité fragmenty riešia aktuálny incident a technológiu
Podloženosť	Podiel tvrdení podporených citáciou; entailment review	Kľúčové kroky majú dohľadateľný zdroj alebo sú označené ako hypotéza
Správnosť postupu	Runbook conformance, expert acceptance rate	Návrh nepreskakuje bezpečnostné a schvaľovacie kroky
Bezpečnosť	Adversarial test, prompt injection, data exfiltration	Nedôveryhodný obsah nemení systémové pravidlá ani rozsah oprávnení
Užitočnosť	Čas do rozhodnutia, miera prijatia/úpravy	Odporúčanie znižuje kognitívnu záťaž bez straty kontroly

4.4 Životný cyklus AI modelu a riadenie zmien

AI komponent sa nesmie spravovať ako statická knižnica. Každá nasadená verzia musí byť spätne priraditeľná k dátam, konfigurácii, promptom, hodnotiacim sadám a schvaľovaciemu rozhodnutiu. Riadenie životného cyklu zároveň oddeľuje kvalitu modelu od oprávnení, politiky vykonania a prevádzkových bezpečnostných hraníc.

Fáza	Povinný artefakt	Kontrolná brána
Dátová príprava	Verzia datasetu, pôvod, právny režim, profil kvality a rozdelenie train/validation/test	Testovacia množina zostáva oddelená od tréningu, ladenia promptov aj voľby prahov
Vývoj a evaluácia	Model, konfigurácia, šablóny promptov, golden set a metriky podľa use-case	Vopred určené prahy relevantnosti, podloženosti, bezpečnosti a latencie
Schválenie a nasadenie	Model card, register verzií, rozhodnutie o vydaní a plán shadow/canary nasadenia	Nasadzuje sa iba schválená verzia; AI návrh nemôže obísť politiku oprávnení
Prevádzka	Monitoring dátového a modelového driftu, kvality výstupov, latencie, chýb a nákladov	Prekročenie prahov vyvolá alarm, obmedzenie funkcie alebo fallback bez AI
Zmena alebo rollback	Dôvod zmeny, rozsah revalidácie, porovnanie s referenčnou verziou a rollback point	Významná zmena dát, modelu alebo promptov vyvolá primeranú revalidáciu

5. Automatizácia expertného know-how

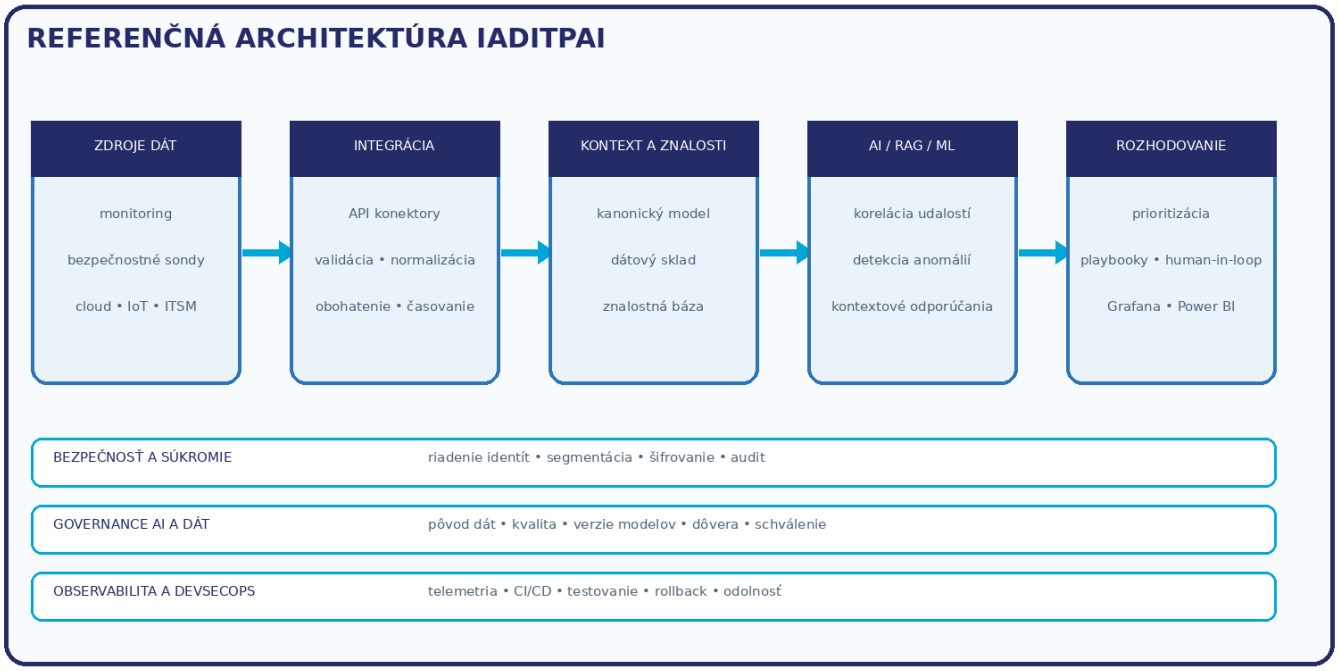
Seniorné know-how sa v praxi nachádza v runbookoch, tiketoch, konfiguráciách a implicitných rozhodovacích návykoch. Jeho prenos vyžaduje viac než vloženie dokumentov do vyhľadávača. Každá znalostná jednotka musí mať vlastníka, rozsah použiteľnosti, predpoklady, rizikovosť, platnosť, verziu a spôsob testovania.

Forma znalosti	Vhodné použitie	Governance
Pravidlo	Jednoznačná podmienka a reakcia; napr. korelácia známej kombinácie signálov	Peer review, test fixtures, verzia a rollback
Rozhodovací strom	Diagnostika s rozvetvením podľa pozorovaní	Úplnosť vetiev, vlastník a pravidelná revízia
Playbook	Viackrokový postup s rolami, bránami a dôkazmi	Schválenie, least privilege, simulácia a záznam vykonania
Znalostný dokument	Kontext, vysvetlenie, výnimky a obmedzenia	Metadáta, ACL, účinnosť, citovateľné fragmenty
Modelový vzor	Štatistické rozpoznanie anomálie alebo klasifikácia	Dátový pôvod, metriky, drift a revalidácia

Human-in-the-loop Človek nie je iba posledné tlačidlo. Musí vidieť fakty, neistotu, alternatívy a dôsledky; má možnosť odporúčanie prijať, upraviť, odmietnuť alebo eskalovať a spätná väzba sa nesmie automaticky stať tréningovou pravdou bez kontroly.

6. Referenčná architektúra a hranice dôvery

Referenčná architektúra oddeľuje päť funkčných zón a tri prierezové kontrolné vrstvy. Tok zľava doprava predstavuje spracovanie od zdrojového signálu po rozhodovací výstup. Každý prechod je rozhraním s vlastným kontraktom, identitou, auditom a chybovým režimom.



Obrázok 1 – Referenčná architektúra IADITPAI. Šípky znázorňujú riadený tok dát a kontextu; prierezové vrstvy platia pre všetky zóny.

Architektonické zóny

Zóna	Zodpovednosť	Hranica dôvery
Zdroje dát	Vytvoriť autentický signál a sprístupniť ho definovaným rozhraním.	Zdroj je externý voči jadru; obsah je nedôveryhodný, kým neprejde validáciou.
Integrácia	Prijať, overiť, normalizovať, deduplikovať, obohatiť a trasovať.	Každý konektor má samostatnú identitu, oprávnenia a rate limit.
Kontext a znalosti	Uchovať kanonické udalosti, väzby, históriu, dokumenty a pôvod.	ACL platí pri zápise aj retrieval; index nesmie obísť prístupové pravidlá.
AI / RAG / ML	Korelovať, detegovať anomálie, vyhľadať oporu a zostaviť odporúčanie.	Prompt, model a externý obsah nie sú autoritou pre vykonanie privilegovanej akcie.
Rozhodovanie	Prioritizovať, zobraziť, schváliť, eskalovať alebo spustiť povolený playbook.	Akcia vyžaduje politiku, oprávnenie, kontrolu parametrov a audit.

6.1 Prevádzkové varianty

Variant	Vhodnosť	Podmienky
On-prem	Regulované prostredie, vysoká citlivosť dát, integrácia s lokálnymi systémami	Lokálny model alebo kontrolovaný inference endpoint; lokálne logy a znalostná báza
Hybrid	Časť spracovania lokálne, škálovateľné modelové služby mimo prostredia	Minimalizácia a pseudonymizácia vstupu, egress politika, zmluvná a technická kontrola
PaaS	Organizácie s nižšou citlivosťou a požiadavkou na rýchle škálovanie	Tenant isolation, šifrovanie, regionálne uloženie, export a ukončenie služby

7. Dátový a rozhodovací životný cyklus

Životný cyklus musí zabezpečiť, že rovnaká vstupná udalosť a rovnaká verzia pravidiel vytvoria reprodukovateľný medzivýsledok. Generatívna časť môže byť pravdepodobnostná, preto sa reprodukovateľnosť opiera o uloženie vstupného kontextu, identifikátorov retrievalu, verzie modelu a parametrov, nie o predpoklad identického textu.

Fáza	Dôkaz / záznam	Kontrolná otázka
1. Ingest	ID zdroja, čas, hash alebo referencia originálu	Vieme dokázať, čo zdroj skutočne poslal?
2. Validate	Výsledok schémy, autentizácie a kvality	Bola chybná udalosť izolovaná bez straty?

Fáza	Dôkaz / záznam	Kontrolná otázka
3. Normalize	Verzia mapovania a kanonický záznam	Zachoval sa význam, jednotky a čas?
4. Enrich	Zdroj topológie, vlastník, kritickosť, zmena	Je obohatenie fakt alebo neistý odhad?
5. Correlate	Skupina udalostí, okno, pravidlo/model	Prečo boli signály spojené alebo potlačené?
6. Retrieve	ID a verzia fragmentov, skóre a ACL	Mal používateľ právo vidieť každý zdroj?
7. Infer	Model, parametre, prompt template, confidence	Je fakt oddelený od hypotézy?
8. Decide	Rola, politika, schválenie/odmietnutie	Kto prevzal zodpovednosť za akciu?
9. Act & verify	Playbook, parametre, výsledok, rollback	Bol dosiahnutý očakávaný stav bez vedľajšieho dopadu?
10. Learn	Spätná väzba, review a schválená aktualizácia	Bola skúsenosť validovaná pred opätovným použitím?

Nemennosť dôkazov Zdrojová udalosť a auditný záznam sa neopravujú prepísaním. Oprava vzniká ako nový, previazaný záznam, aby bolo možné spätne vysvetliť rozhodnutie platné v danom čase.

8. Vizualizácia a Human-Centered AI

Jednotná platforma nesmie znamenať jednotný dashboard pre všetkých. Operátor potrebuje časovú blízkosť, drill-down, technický kontext a rýchlu odozvu. Manažment potrebuje trendy, vývoj rizika, SLA, náklady a porovnanie období. Grafana a Power BI preto plnia komplementárne roly nad spoločným významovým a autorizačným základom.

Persona	Rozhodnutie	Preferovaný pohľad	Ochrana pred chybou
L1 operátor	Je potrebná okamžitá eskalácia?	Prioritný incident, dôvod, základné kroky, vlastník	Jednoznačná závažnosť, zákaz skrytých automatických akcií
L2/L3 špecialista	Aká je koreňová príčina a bezpečný zásah?	Surové signály, topológia, zmeny, citácie, alternatívy	Zobrazenie neistoty, provenance a rollbacku
Bezpečnostný tím	Ide o hrozbu a aký je rozsah?	Korelácia identít, aktív, indikátorov a časovej osi	Least privilege, dôkazná stopa, oddelenie tenantov
Manažment	Kde rastie riziko alebo náklad?	Trend KPI, SLA, kapacita, náklad, využitie technológií	Agregácia, definícia metriky, zákaz neoverených kauzálnych tvrdení
Audítor	Je rozhodnutie dohľadateľné a v súlade s politikou?	Read-only časová os, verzie artefaktov a schválenia	Nemennosť záznamu a kontrola exportu

Použiteľnosť sa overuje na scenároch, nie iba dotazníkom spokojnosti. Meria sa čas do identifikácie incidentu, počet krokov, miera nesprávnych interpretácií, úspešnosť nájdenia zdroja odporúčania a schopnosť používateľa rozlíšiť fakt, odhad a generovaný návrh.

9. Bezpečnosť, súkromie a dátová suverenita

IADITPAI centralizuje kontext, nie nevyhnutne všetky surové dáta. Bezpečnostný model predpokladá kompromitáciu jednotlivého konektora, chybné alebo útočné dáta, zneužitie retrievalu aj nespoľahlivý výstup modelu. Obrana je vrstvená: segmentácia, identity pracovných záťaží, minimálne oprávnenia, šifrovanie, audit, validácia vstupu a výstupu, ochrana tajomstiev a riadenie dodávateľského reťazca.

Oblasť	Minimálna kontrola	Evidencia
Identita a prístup	RBAC/ABAC, MFA pre administráciu, workload identity, short-lived credentials	Matica rolí, access review, autentizačné logy
Sieť a rozhrania	Segmentácia, allow-list, mTLS/TLS, rate limiting, schema validation	Diagram tokov, pravidlá firewallu, API testy
Dáta	Klasifikácia, minimalizácia, šifrovanie, retencia a bezpečný výmaz	Register dát, DPIA podľa potreby, retenčné politiky
Znalostná báza	ACL pred retrievalom, schválené zdroje, ochrana pred poisoningom	Index lineage, vlastníci dokumentov, revízne záznamy

Oblasť	Minimálna kontrola	Evidencia
Model	Registry, schválená verzia, evals, monitoring driftu, fallback	Model card, eval report, release decision
Tajomstvá	Vault, rotácia, zákaz tajomstiev v promptoch a logoch	Scan repozitára/logov, rotácia a incidentný postup
Audit	Trace od udalosti po odporúčanie a akciu; synchronizovaný čas	Nemenné alebo append-only záznamy, export pre audit

9.1 Súkromie a minimalizácia

Prevádzkové dáta môžu nepriamo obsahovať osobné údaje – používateľské mená, IP adresy, identifikátory zariadení alebo obsah tiketov. Pred spracovaním sa určí účel, právny základ, nevyhnutný rozsah, retencia a príjemcovia. Pseudonymizácia alebo tokenizácia sa vykonáva pred odoslaním do komponentu, ktorý danú identitu nepotrebuje. Verejné a zákaznícke znalosti sa logicky aj autorizačne oddeľujú.

10. DevSecOps, pozorovateľnosť a prevádzková odolnosť

Kvalita systému nevzniká jednorazovým penetračným testom. DevSecOps pipeline spája kontrolu zdrojového kódu, závislostí, infraštruktúry, kontajnerov, tajomstiev, dátových schém a AI artefaktov. Každé vydanie má dohľadateľnú zostavu, testovací protokol, schválenie a plán návratu.

Brána	Automatizovaná kontrola	Manuálne rozhodnutie
Commit / merge	Lint, unit test, SAST, secret scan, schema test	Peer review a vlastníctvo zmeny
Build	Pinned dependencies, SBOM, podpis artefaktu, malware scan	Akceptácia kritickej výnimky
Integrácia	Contract test konektorov, integračný test, syntetické dáta	Posúdenie zmeny dátového významu
AI evaluation	Golden set, groundedness, harmful output, injection test	Odborné hodnotenie hraničných prípadov
Pre-production	DAST, performance, resilience, backup/restore	Go/no-go a potvrdenie rollbacku
Produkcia	SLO, drift, kvalita dát, alerty, canary	Incident review a rozhodnutie o revalidácii

10.1 SLO a degradačné režimy

- Výpadok jedného konektora: izolovať tok, zachovať ostatné zdroje, zobraziť dátovú neúplnosť a po obnove vykonať kontrolovaný replay.
- Výpadok modelu alebo retrievalu: pokračovať v zbere a pravidlovej korelácii; AI odporúčanie označiť ako nedostupné, nie nahradiť neovereným odhadom.
- Nárast latencie: aplikovať backpressure, prioritizovať kritické udalosti, zachovať poradie tam, kde je významné, a merať end-to-end oneskorenie.
- Zhoršenie dátovej kvality alebo drift: znížiť dôveru, aktivovať alarm a revalidovať mapovanie/model pred automatizovaným použitím.

11. Model hrozieb

Model hrozieb posudzuje aktíva – konektory, surové a normalizované dáta, znalostnú bázu, modely, prompt šablóny, politiky, audit a akčné rozhrania. Útočníkom môže byť externý aktér, kompromitovaný zdroj, používateľ s nadmernými oprávneniami alebo dodávateľský artefakt. Chybný výstup bez útočníka sa posudzuje rovnako disciplinovane ako bezpečnostná hrozba.

Hrozba	Scenár	Kontroly	Reziduálne riziko
Data poisoning	Zdroj alebo import vloží zavádzajúce udalosti či znalosti.	Autentizácia, provenance, karanténa, schválené zdroje, anomálie kvality	Dôveryhodný zdroj môže poskytnúť vecne chybný údaj.
Prompt / retrieval injection	Dokument prikazuje modelu obísť pravidlá alebo odhaliť dáta.	Oddelenie inštrukcií a obsahu, ACL, sanitizácia, allow-list nástrojov	Nové obfuskačné techniky vyžadujú priebežné red-team testy.
Halucinácia	Model vytvorí neexistujúcu príčinu alebo riskantný krok.	Citácie, groundedness, confidence, šablóna, human approval	Presvedčivý jazyk môže ovplyvniť používateľa aj pri označení neistoty.
Privilege escalation	Odporúčanie alebo playbook spustí akciu mimo roly.	Policy enforcement mimo modelu, least privilege, parameter validation	Chyba v integračnej službe alebo politike.

Hrozba	Scenár	Kontroly	Reziduálne riziko
Schema drift	Zmena zdroja potichu zmení význam údajov.	Contract test, verzia schémy, canary a kvalitatívne metriky	Sémantická zmena bez technickej zmeny schémy.
Únik dát	Citlivý obsah sa dostane do promptu, logu alebo cudzieho tenantu.	Minimalizácia, DLP, redaction, tenant isolation, egress policy	Neúplná klasifikácia vo voľnom texte.
Model drift	Výkon sa zhorší po zmene prostredia alebo správania.	Baseline, monitoring distribúcie a outcome, revalidácia, rollback	Oneskorená spätná väzba pri zriedkavých incidentoch.
DoS / resource exhaustion	Tok udalostí alebo nákladné dotazy vyčerpajú kapacitu.	Rate limit, queue, priority, budget, circuit breaker	Extrémna udalosť môže znížiť úplnosť v kritickom čase.

12. Validačný rámec a prechod TRL 3 → TRL 8

Východiskový TRL 3 znamená experimentálne overené analytické princípy a čiastočné komponenty bez integrovaného systému. Cieľový TRL 8 vyžaduje kompletný a kvalifikovaný systém overený v reálnych podmienkach. Prechod sa preto nepreukazuje jedinou demonštráciou, ale reťazcom dôkazov od požiadavky cez test po výsledok pilota.

Úroveň	Dôkaz pripravenosti	Exit kritérium
TRL 3	Overené princípy integrácie, analýzy a AI na izolovaných príkladoch	Formulované hypotézy, riziká a merateľné požiadavky
TRL 4–5	Komponenty a laboratórna integrácia na reprezentatívnych dátach	Konektory, schéma, AI pipeline a bezpečnostné kontroly prejdú modulovými testmi
TRL 6	Funkčný integrovaný prototyp	End-to-end scenár od zdroja po auditované odporúčanie
TRL 7	Pilot v relevantnom prostredí	Stabilita, výkon, použiteľnosť a bezpečnosť pri reálnych obmedzeniach
TRL 8	Kompletný kvalifikovaný systém v reálnych podmienkach	Akceptačné kritériá, prevádzková dokumentácia, KPI a riadené reziduálne riziká

12.1 Validačné domény

Doména	Príklad merania	Minimálny dôkaz
Funkčnosť	Úspešnosť ingestu, mapovania, korelácie a workflow	Test prípady s očakávaným výsledkom a trace
Kvalita dát	Úplnosť, platnosť, duplicity, oneskorenie, lineage coverage	Profil dát pred/po transformácii
AI/RAG	Precision/recall, relevance@k, groundedness, expert acceptance	Golden set, metodika anotácie a výsledky podľa use-case
Výkon	Throughput, p95/p99 latencia, backlog a čas replay	Load test v reprezentatívnej konfigurácii
Odolnosť	RTO/RPO, failover, degradácia, obnova konektora	Chaos/failure scenáre a protokol obnovy
Bezpečnosť	Zraniteľnosti, prístup, izolácia, prompt injection, egress	Threat model, test report a uzavretie nálezov
Použiteľnosť	Task success, čas, počet krokov, chybovosť interpretácie	Test s IT aj non-IT používateľmi
Prevádzkový prínos	MTTD/MTTR, alert fatigue, využitie nástrojov, onboarding	Baseline, porovnateľné obdobie a vysvetlenie odchýlok

12.2 Cieľové KPI a pravidlá interpretácie

KPI	Projektová hypotéza	Výpočet / podmienka
MTTD/MTTR	Skrátenie o 30–50 %	Porovnanie mediánu a percentilov rovnakých tried incidentov voči baseline
Náklady na špecialistov	Zníženie o 20–30 %	Čas rolí × jednotkový náklad; oddeliť implementáciu od bežnej prevádzky
Využitie existujúcich technológií	Nárast z 30–40 % na >70 %	Podiel dostupných relevantných dát/funkcií zapojených do rozhodovacích scenárov
Nerelevantné alerty	Zníženie o 40 %	Podiel alertov uzavretých ako neakčné; sledovať aj false negatives
Onboarding technológie	Skrátenie o 25–35 %	Čas od dostupného rozhrania po akceptovaný konektor a dashboard

12.3 Metodika pilotného merania

Cieľové intervaly KPI sú projektové hypotézy, kým ich nepotvrdí reprodukovateľné pilotné meranie. Protokol musí vzniknúť pred vyhodnotením, zachovať porovnateľnosť vzoriek a uviesť aj negatívne alebo nejednoznačné výsledky. Ak počet pozorovaní umožňuje štatistické vyhodnotenie, bodový odhad sa doplní intervalom neistoty.

Krok	Metodické pravidlo	Minimálny dôkaz
Baseline	Vopred určiť obdobie, záťaž systému, taxonómiu incidentov, workflow a význam každej metriky	Baseline protokol a export zdrojových záznamov
Porovnateľná vzorka	Porovnávať rovnaké triedy incidentov; zdôvodniť vyradenia, outliery a minimálny počet prípadov	Register vzorky s kritériami zaradenia a vyradenia
Meranie	Popri priemere uviesť medián a relevantné percentily; merať aj task success a závažné zlyhania	Časovo označené záznamy, exporty nástrojov a opakovateľný výpočet
Rušivé vplyvy	Oddeliť účinok platformy od zmien personálu, nástrojov, školenia, procesov a skladby incidentov	Záznam zmien a odborná interpretácia ich vplyvu
Akceptácia	Výsledky porovnať s vopred určenými prahmi a zdokumentovať odchýlky, neistotu a reziduálne riziká	Hodnotiaca správa s väzbou na výskumné otázky, KPI a exit kritériá TRL

13. Súlad s normami, reguláciou a stratégiami

Použité rámce nie sú certifikátom ani automatickým dôkazom súladu. Slúžia ako zdroj overiteľných požiadaviek a kontrolných otázok. Konkrétna právna kvalifikácia závisí od nasadenia, typu spracúvaných údajov, roly organizácie a rozsahu automatizovaného rozhodovania.

Rámec	Význam pre IADITPAI	Praktické premietnutie
ISO/IEC 25010:2023	Model kvality ICT a softvérového produktu	Požiadavky a testy funkčnosti, výkonnosti, kompatibility, bezpečnosti, udržateľnosti a ďalších atribútov
ISO 9241-210 / Human-Centred Design	Proces návrhu interaktívnych systémov okolo používateľov a úloh	Persony, participatívny návrh, scenáre a testovanie použiteľnosti
ISO/IEC 27001	Systémové riadenie informačnej bezpečnosti	Aktíva, riziká, kontroly, incidenty, dodávatelia a dôkazy
GDPR	Zásady zákonnosti, minimalizácie, bezpečnosti a práv dotknutých osôb	Klasifikácia dát, účel, retencia, prístup a posúdenie vplyvu podľa potreby
NIS2	Riadenie kybernetických rizík a odolnosti pre relevantné subjekty	Incident management, kontinuita, dodávateľský reťazec, bezpečný vývoj a reporting
NIST AI RMF 1.0	Dobrovoľný rámec dôveryhodnej a zodpovednej AI	Govern, Map, Measure, Manage; evidencia rizík a meraní počas životného cyklu
NIST SSDF 1.1 + 800-218A	Bezpečný životný cyklus softvéru a rozšírenie pre AI modely	Príprava, ochrana, produkcia bezpečného softvéru a reakcia na zraniteľnosti
FAIR a otvorené API	Nájditeľnosť, dostupnosť, interoperabilita a opätovná použiteľnosť	Metadáta, identifikátory, verzovanie a zdokumentované rozhrania v primeranom rozsahu
RIS3 SK 3-2	Zvyšovanie úžitkovej hodnoty údajov a databáz	Agregácia, kontextualizácia a rozhodovacia hodnota heterogénnych IT dát

14. Scenáre nasadenia

Scenár	Primárna hodnota	Špecifické obmedzenie
MSP / systémový integrátor	Korelácia naprieč zákazníkmi, štandardizované playbooky a rýchly onboarding	Prísna tenant isolation a oddelenie znalostí
Verejná správa	Zjednotenie heterogénnych nástrojov a manažérske reportovanie	On-prem, auditovateľnosť, verejné obstarávanie a dlhá životnosť systémov

Scenár	Primárna hodnota	Špecifické obmedzenie
Zdravotníctvo	Prevádzková dostupnosť, prioritizácia incidentov a ochrana citlivých údajov	Minimalizácia, segmentácia a vysoká požiadavka na kontinuitu
Kritická infraštruktúra	Spoločný kontext IT/OT a bezpečnostných udalostí	Oddelenie zón, deterministické kontroly a obmedzená automatizácia
Priemysel / IoT	Korelácia telemetrie, kvality a údržby	Objem dát, edge spracovanie, nejednotné protokoly
Cloud a dátové centrá	Kapacitné, nákladové a bezpečnostné súvislosti	Dynamická topológia, egress náklady a viac účtov/tenantov

Nasadenie sa začína katalógom zdrojov, rolí a rozhodnutí. Nasleduje jeden prioritný use-case s merateľnou baseline, potom rozšírenie konektorov a znalostí. Takýto fázový postup obmedzuje integračné riziko a zároveň umožňuje oddeliť prínos platformy od súbežných organizačných zmien.

15. Riziká a otvorené výskumné otázky

Riziko / otázka	Dopad	Mitigácia / ďalší experiment
Nekonzistentná sémantika zdrojov	Falošná korelácia alebo neporovnateľné KPI	Kanonický model, dátové kontrakty, domain steward a test významu
Nedostatok reprezentatívnych incidentov	Nadhodnotená presnosť a slabá generalizácia	Syntetické scenáre, historický replay, expert review, confidence intervals
Expert bias v kodifikovanom know-how	Automatizácia zastaraného alebo jednostranného postupu	Viacnásobný review, dátum platnosti, alternatívy a spätná väzba
Nejasné vlastníctvo dát/modelu	Pomalé opravy, konfliktné pravidlá a auditné medzery	RACI, registry vlastníkov, schvaľovacie workflow a SLA
Vendor lock-in modelu alebo cloudu	Nákladný prechod a obmedzená dátová suverenita	Abstrakčná vrstva, exportné formáty, lokálne varianty a test portability
Automatizačný bias používateľa	Akceptovanie presvedčivého, ale nesprávneho návrhu	Vysvetlenie, neistota, nútená kontrola kritických krokov a školenie
Krátke projektové obdobie	Nedostatočný čas na stabilitu a pilotné meranie	Prioritizácia kritických use-case, inkrementálne dôkazy, jasné akceptačné kritériá
Udržateľnosť po projekte	Zastaranie konektorov, znalostí a modelov	Licenčný a servisný model, dokumentácia, školenia, monitoring driftu

15.1 Otvorené otázky pre nadväzujúci výskum

- Ako kalibrovať mieru dôvery tak, aby bola porovnateľná medzi pravidlovou koreláciou, ML skóre a generovaným odporúčaním?
- Ako merať pridanú hodnotu kontextu oddelene od zlepšenia samotných zdrojových nástrojov a procesov tímu?
- Ktoré triedy incidentov sú vhodné na poloautomatizáciu a ktoré musia zostať striktne poradenské?
- Ako preniesť znalosti medzi zákazníkmi bez prenosu citlivého kontextu a bez degradácie významu?
- Ako dlhodobo udržať kvalitu konektorov pri sémantických zmenách API a rýchlom vývoji AI modelov?

16. Väzba na pracovné balíky, míľniky a výstupy

Projektová dokumentácia pracuje s piatimi logickými pracovnými balíkmi a zároveň s piatimi vecnými míľnikmi. Nasledujúca matica spája odborný obsah publikácie s implementačnou a dôkaznou stopou projektu.

WP / míľnik	Hlavný výstup	Väzba na kapitoly	Dôkaz splnenia
WP1 / M1–M2	Aplikačný základ, dátový sklad, architektúra a konektory	1–3, 6–7	Technický návrh, schémy, rozhrania, funkčný prototyp a contract testy
WP2 / M3	AI analytická vrstva, RAG/ML a automatizácia know-how	4–5, 11–12	Modelové artefakty, evals, pravidlá, playbooky a bezpečnostné testy
WP3 / M5	Grafana a Power BI pohľady pre IT aj non-IT používateľov	8	Prototypy, usability testy a akceptované dashboardy
WP4 / M3–M5	Pilotné nasadenia a meranie KPI	10–12, 14	Pilotný protokol, baseline, výsledky, incidenty a akceptácia

WP / míľnik	Hlavný výstup	Väzba na kapitoly	Dôkaz splnenia
WP5	Udržateľnosť, dokumentácia, školenia a diseminácia	13, 15–18	Licenčný/servisný model, školiace materiály a odborná publikácia

Publikačný výstup Tento white paper predstavuje odbornú publikáciu vytvorenú v rámci projektu.

17. Záver

IADITPAI rieši praktický problém fragmentovaných IT dát a nedostatku expertných kapacít architektúrou, ktorá chráni existujúce investície a pridáva nad ne spoločný kontext. Technická hodnota nespočíva v samotnom nasadení generatívneho modelu, ale v riadenej kombinácii dátových kontraktov, proveniencie, korelácie, RAG, strojového učenia, kodifikovaného know-how, ľudskej kontroly a auditovateľného rozhodovania.

Referenčný návrh kladie dôraz na vendor neutralitu, on-prem predvolené spracovanie, oddelenie faktu od inferencie a fail-safe prevádzku. Takéto invarianty umožňujú meniť konkrétne zdrojové nástroje alebo modely bez straty jadra riešenia. Zároveň vytvárajú testovateľnú hranicu medzi poradenskou AI a privilegovanou produkčnou akciou.

Cieľ TRL 8 je vierohodný iba vtedy, ak bude podložený reťazcom dôkazov z relevantného a reálneho prostredia: funkčnosťou, dátovou kvalitou, výkonom, bezpečnosťou, odolnosťou, použiteľnosťou a prevádzkovým prínosom. KPI sa preto interpretujú ako experimentálne hypotézy s definovanou baseline, nie ako izolované percentá. Výsledkom je platforma pripravená na zodpovedné nasadenie a ďalšie rozširovanie do sektorov, kde je kontext, dátová suverenita a auditovateľnosť rozhodujúca.

18. Normatívne a odborné zdroje

[1] ISO/IEC 25010:2023. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model.

[2] ISO 9241-210:2019. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.

[3] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[4] European Parliament and Council. Regulation (EU) 2016/679 (General Data Protection Regulation).

[5] European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2).

[6] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, 2023. DOI: 10.6028/NIST.AI.100-1.

[7] NIST. Secure Software Development Framework (SSDF) Version 1.1, NIST SP 800-218, 2022. DOI: 10.6028/NIST.SP.800-218.

[8] NIST. Secure Software Development Practices for Generative AI and Dual-Use Foundation Models, NIST SP 800-218A, 2024. DOI: 10.6028/NIST.SP.800-218A.

[9] Wilkinson, M. D. et al. The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data 3, 160018 (2016). DOI: 10.1038/sdata.2016.18.

[10] OECD. Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development. OECD Publishing, Paris.

Elektronické odkazy

ISO/IEC 25010:2023 — https://www.iso.org/standard/78176.html

GDPR – EUR-Lex — https://eur-lex.europa.eu/eli/reg/2016/679/oj

NIS 2 – EUR-Lex — https://eur-lex.europa.eu/eli/dir/2022/2555/oj

NIST AI RMF 1.0 — https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

NIST SP 800-218 SSDF — https://csrc.nist.gov/pubs/sp/800/218/final

NIST SP 800-218A — https://csrc.nist.gov/pubs/sp/800/218/a/final

Príloha A – Slovník pojmov

Pojem	Význam v publikácii
AI	Softvérová funkcia využívajúca model alebo pravidlá na klasifikáciu, koreláciu, predikciu či generovanie odporúčania.
RAG	Retrieval-Augmented Generation; generovanie odpovede s využitím vyhľadaných, identifikovateľných znalostných fragmentov.
Kanonický model	Spoločná sémantická reprezentácia udalostí nezávislá od konkrétneho zdrojového nástroja.
Proveniencia / lineage	Pôvod dát a sled transformácií od zdrojového záznamu po odvodený výstup.
Groundedness	Miera, v akej je generované tvrdenie podložené poskytnutými zdrojmi a pozorovanými faktmi.
Human-in-the-loop	Riadené zapojenie človeka do posúdenia, schválenia, úpravy alebo odmietnutia odporúčania či akcie.
MTTD / MTTR	Mean Time to Detect / Mean Time to Restore; ak sa MTTR používa vo význame Resolve alebo Recover, význam musí byť v protokole merania výslovne uvedený.
TRL	Technology Readiness Level; úroveň technologickej pripravenosti od konceptu po kvalifikovaný systém.
SLO	Service Level Objective; merateľný cieľ dostupnosti, latencie, kvality alebo inej prevádzkovej vlastnosti.
SBOM / MBOM	Software Bill of Materials / Model Bill of Materials (MBOM – pracovné označenie v tejto publikácii); evidencia komponentov, modelov, dátových závislostí a ich verzií.
Vendor-agnostic	Návrh, ktorý udržiava jadro funkcie nezávislé od jedného výrobcu alebo proprietárnej dátovej schémy.
Alert fatigue	Znížená schopnosť reagovať v dôsledku veľkého množstva opakovaných alebo málo relevantných upozornení.

Vyhlásenie o pôvode a použití

Publikácia bola vytvorená pre projekt 17I04-04-V05-00017 na základe projektovej zmluvy, jej dodatku a poslednej žiadosti o zmenu. Jej odborná štruktúra je prispôsobená účelu diseminácie výsledkov projektu TYRON COMPANY, s. r. o. Vizuálny systém nadväzuje na referenčný white paper projektu DecentraSafe, avšak technický obsah, architektúra, riziká, KPI a závery sú spracované pre potreby projektu IADITPAI.

Odporúčaná citácia TYRON COMPANY, s. r. o. (2026). IADITPAI: Integrovaná a agregovaná dátová IT platforma využívajúca umelú inteligenciu. Odborný white paper. Projekt 17I04-04-V05-00017. Cabaj – Čápor.