PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

V29 záverečná správa projektu

KPB9 – záverečná správa

typ – report

mesiac odovzdania – M24

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. Manažérske zhrnutie 3
2. Zhrnutie naplnenia cieľov v definovanom časovom období 3
3. Zhrnutie dodaných výstupov v definovanom časovom období 4
4. Zhrnutie hlavných udalostí a rizík 6
5. Najdôležitejšie poučenia a odporúčania pre ďalšie smerovanie 7

1. MANAŽÉRSKE ZHRNUTIE

Záverečná správa bola vypracovaná k mesiacu M24 – k finálnemu ukončeniu projektu. Vypracovala sa v spolupráci projektových manažérov za oboch partnerov (FRI, BRAIN:IT). Obsahuje 5 základných častí a podklady pre jej vypracovanie boli zaslané lídrami všetkých pracovných balíkov.

Cieľom projektu bolo navrhnúť a implementovať bezpečnostné operačné centrum ako cloudovú službu, ktorá využíva princípy multitenantnosti a prvky strojového učenia na zlepšenie detekcie a reakcie na kybernetické hrozby.

Správa sumarizuje výstupy a pokrok dosiahnutý v období **apríl 2024 (M1) až marec 2026 (M24).** Podrobne dokumentuje 29 výstupov vrátane analýz, návrhov komponentov, kritérií, logického rámca, technologickej architektúry a monitorovacích mechanizmov.

2. ZHRNUTIE NAPLNENIA CIEĽOV V DEFINOVANOM ČASOVOM OBDOBÍ

Hlavným cieľom projektu bolo: návrh otvoreného, multitenantného riešenia operačného centra bezpečnosti SOC, ktoré bude poskytované ako výkonovo flexibilná cloudová/kontajnerová služba s modulmi pre detekciu a predikciu anomálii s využitím strojového učenia a neurónových sietí. Pre zabezpečenie dosiahnutia hlavného cieľa projektu bolo identifikovaných päť **špecifických cieľov projektu**:

1. Návrh technologického riešenia pre prevádzkovanie služby SOC s využitím virtualizovaných riešení spracovanom až na úroveň TRL3.
2. Návrh inteligentného systému pre monitoring technologických prostriedkov a služieb.
3. Návrh architektúry samotnej inovatívnej elastickej služby INNOSOC ako integrácie otvorených riešení a komponentov.
4. Návrh vhodných algoritmov strojového učenia s aplikáciou hlbokých neurónových sietí pre riešenie úlohy detekcie a predikcie bezpečnostných a operačných anomálií.
5. Vytvorenie platformy pre zdieľanie nadobudnutých poznatkov v zmysle realizovaného projektu a zásad otvorenej vedy.

Dosahovanie čiastkových cieľov bolo realizované vykonávaním aktivít v rámci pracovných balíkov, ktoré boli s jednotlivými cieľmi prepojené. Naplnenie všetkých čiastkových cieľov viedlo k naplneniu hlavného cieľa celého projektu. Návrh multitenantného riešenia operačného centra bezpečnosti SOC bol vytvorený.

Naplnenie cieľov sa odvíjalo aj od vytvorenia a dodania špecifikovaných výstupov (V1-V29). Odovzdanie niektorých z nich bolo na základe opodstatnených dôvodov posunuté v čase, čo ale neovplyvnilo naplnenie cieľov k ukončeniu projektu. Posunuté termíny odovzdania dotknutých výstupov sú zachytené v nasledujúcej časti (tabuľka 1).

3. ZHRNUTIE DODANÝCH VÝSTUPOV V DEFINOVANOM ČASOVOM OBDOBÍ

V tabuľke 1 sa nachádzajú výstupy z obdobia M1-M24 spolu s plánovaným aj reálnym termínom ich dodania. Tieto boli sumarizované na základe výstupu *V25 časové dispozície projektu* a *V28 priebežná správa projektu* a následne bol ďalší progres monitorovaný a vyhodnotení ku koncu mesiacu M24 pri vytváraní tejto záverečnej správy.

Tabuľka 1 Výstupy za stanovené obdobie

Číslo výstupu	Výstup	Kód pracovného balíka	Subjekt zodpovedný za výstup	Typ	Spôsob overenia	Dodanie výstupu – plánovaný (mesiac projektu)	Dodanie výstupu – reálny (mesiac projektu)
V1	výsledok analýzy dostupných riešení	KPB1	UNIZAFRI	dokumentácia	kompletná dokumentácia	M3 (jún 24)	M3 (jún 24)
V2	zoznam definovaných kritérií	KPB1	UNIZAFRI	zoznam	schválený zoznam	M5 (aug 24)	M5 (aug 24)
V3	popis vybraného riešenia spĺňajúceho stanovené kritériá	KPB1	UNIZAFRI	dokumentácia	kompletná dokumentácia	M7 (okt 24)	M7 (okt 24)
V4	výsledok analýzy vhodných komponentov	KPB2	UNIZAFRI	dokumentácia	kompletná dokumentácia	M3 (jún 24)	M3 (jún 24)
V5	zoznam definovaných kritérií	KPB2	UNIZAFRI	zoznam	schválený zoznam	M5 (aug 24)	M5 (aug 24)
V6	popis dashbordov, monitorovacieho a reportovacieho systému	KPB2	UNIZAFRI	dokumentácia	kompletná dokumentácia	M7 (okt 24)	M7 (okt 24)
V7	výsledok analýzy vhodných algoritmov	KPB3	UNIZAFRI	dokumentácia	kompletná dokumentácia	M10 (jan 25)	M18 (sept 25)*
V8	zoznam definovaných kritérií	KPB3	UNIZAFRI	zoznam	schválený zoznam	M10 (jan 25)	M18 (sept 25)*
V9	popis vybraného algoritmu spĺňajúceho stanovené kritériá	KPB3	UNIZAFRI	dokumentácia	kompletná dokumentácia	M17 (aug 25)	M18 (sept 25)*
V10	zoznam funkčných a nefunkčných požiadaviek	KPB4	BRAIN:IT	zoznam	schválený zoznam	M14 (máj 25)	M14 (máj 25)
V11	biznis architektúra	KPB4	BRAIN:IT	dokumentácia	schválená dokumentácia	M16 (júl 25)	M16 (júl 25)
V12	technologická architektúra	KPB4	BRAIN:IT	dokumentácia	schválená dokumentácia	M19 (okt 25)	M19 (okt 25)
V13	DNR – detailný návrh riešenia spolu s prílohami	KPB4	BRAIN:IT	dokumentácia	kompletná dokumentácia	M22 (jan 26)	M22 (jan 26)
V14	funkčná infraštruktúra	KPB5	BRAIN:IT	dokumentácia	funkčná infraštruktúra	M19 (okt 25)	M22 (jan 26)**
V15	SW komponenty	KPB5	BRAIN:IT	zoznam	schválený zoznam	M20 (nov 25)	M22 (jan 26)**
V16	funkčný PoC	KPB5	BRAIN:IT	dokumentácia	stabilnáunkčná cloud služba	M22 (jan 26)	M22 (jan 26)
V17	výsledky a vyhodnotenie testov	KPB5	BRAIN:IT	protokol	schválený protokol	M24 (mar 26)	M24 (mar 26)

Číslo výstupu	Výstup	Kód pracovného balíka	Subjekt zodpovedný za výstup	Typ	Spôsob overenia	Dodanie výstupu – plánovaný (mesiac projektu)	Dodanie výstupu – reálny (mesiac projektu)
V18	publikované indexované články v časopisoch	KPB6	UNIZAFRI	články	registrácia v knižnici, indexovanie	M24 (mar 26)	M24 (mar 26)
V19	príspevky z konferencií, zaradené v zborníkoch	KPB6	UNIZAFRI	zborníky	registrácia v knižnici, indexovanie	M24 (mar 26)	M24 (mar 26)
V20	vytvorenie online platformy	KPB7	BRAIN:IT	informačný portál	dostupnosť online	M15 (jún 25)	M15 (jún 25)
V21	dostupné online osvetové podklady a výstupy	KPB7	BRAIN:IT	edukačné materiály	schválený zoznam	M22 (jan 26)	M22 (jan 26)
V22	zrealizované osvetové aktivity	KPB7	BRAIN:IT	aktivity	zoznam účastníkov, fotodokumentácia	M24 (mar 26)	M24 (mar 26)
V23	aktualizované zdôvodnenie projektu	KPB8	UNIZAFRI	dokumentácia	schválené projektovým výborom	M3 (jún 24)	M3 (jún 24)
V24	aktualizovaný logický rámec projektu	KPB8	UNIZAFRI	dokumentácia	schválené projektovým výborom	M3 (jún 24)	M3 (jún 24)
V25	aktualizované nástroje sledujúce časové dispozície projektu a plnenie cieľov	KPB8	UNIZAFRI	dokumentácia	schválené projektovým výborom	M5 (aug 24)	M5 (aug 24)
V26	aktualizované čerpanie stanoveného rozpočtu	KPB8	UNIZAFRI	dokumentácia	schválené projektovým výborom	M6 (sept 24)	M6 (sept 24)
V27	register rizík	KPB8	UNIZAFRI	register	schválené projektovým výborom	M3 (jún 24)	M3 (jún 24)
V28	priebežná správa projektu	KPB8	UNIZAFRI	report	schválené projektovým výborom	M12 (mar 25)	M12 (mar 25)
V29	záverečná správa projektu	KPB9	UNIZAFRI	report	schválené projektovým výborom	M24 (mar 26)	M24 (mar 26)

**Nastalo preťaženie kapacít členov projektového tímu vedúce k posunu vopred nastavených termínov pre výstupy V7, V8, V9. Aplikované bolo opatrenie – zdieľať dopady medzi partnermi zapojenými do projektu. Finalizácia výstupov (V7, V8, V9) bola posunutá na mesiac M18. Partner BRAIN:IT poskytol dodatočnú kapacitu na výpomoc s výstupmi V7 a V8.*

***Vybrané technológie nespĺňajú všetky relevantné definované požiadavky pri záverečnej kontrole pred vstupom do ďalšieho kroku – zmena komerčného statusu komponentu „The Hive“. Musel byť posunutý finálny termín odovzdania výstupov V14 a V15 na mesiac M22. Bol zvolený nový komponent, na základe ktorého sa upravovali výstupy V14 a V15.*

4. ZHRNUTIE HLAVNÝCH UDALOSTÍ A RIZÍK

Počiatočné riziká boli identifikované ku mesiacu M3 v rámci výstupu **V27 register rizík** (KPB8). Tieto boli dopracované do mesiaca M12, kedy sa vytvárala priebežná správa (V28). Preto bol vytvorený dodatok k výstupu V27 s názvom **podklady pre V28_aktualizovaný register rizík k mesiacu M12.** Ten sa podľa potreby priebežne aktualizoval počas celého trvania projektu až do M24. V rámci registra rizík boli identifikované vyvolávajúce udalosti (spúšťače). Za ich monitorovanie bol zodpovedný líder príslušného pracovného balíka.

V rámci priebehu projektu nastali viaceré problémy detegované na základe definovaných vyvolávajúcich udalostí zachytených v registri rizík. Medzi najvýznamnejšie riziká patrili: R7, R9 a R15.

R7 – Nesledovanie úzkych miest na projekte. Spúšťač: Nastalo úzke miesto, ktoré nebolo vopred identifikované. Išlo o preťaženie kapacít členov projektového tímu vedúce k posunu vopred nastavených termínov pre výstupy V7, V8, V9. Neskôr toto isté riziko zasiahlo aj dodávanie výstupov V11, V12.

R9 – Komunikačné nezrovnalosti medzi partnermi. Spúšťač: Došlo ku komunikačnému šumu a opätovné pýtanie si už poskytnutých informácií členmi projektového tímu zapojenými do realizovaných aktivít.

R15 – Chyby v podkladoch pre aktualizované zdôvodnenie projektu. Spúšťač: Odhalená chyba pri preberaní výstupu projektovým manažérom pri míľniku MS1 (viac informácií v časti Míľniky).

R19 – Nesprávny výber technológií pre SOC systém. Spúšťač: Vybrané technológie nespĺňajú všetky relevantné definované požiadavky pri záverečnej kontrole pred vstupom do ďalšieho kroku – reálne prejavenie tohto rizika je spojené so zmenou komerčného statusu komponentu „The Hive“. Musel byť posunutý finálny termín odovzdania výstupov V14 a V15 na mesiac M22.

R25 – Sťažená koordinácia členov tímu počas letných mesiacov (M16, M17) z dôvodu čerpania dovoleniek projektovým tímom.

5. NAJDÔLEŽITEJŠIE POUČENIA A ODPORÚČANIA PRE ĎALŠIE SMEROVANIE

Priebeh projektu potvrdil význam priebežného monitorovania rizík a ich aktualizácie počas celej realizácie. Ukázalo sa, že evidencia rizík v registri je dôležitým základom, avšak rovnako podstatná je schopnosť včas identifikovať ich reálne prejavy, vyhodnocovať dopady na harmonogram a operatívne prijímať vhodné opatrenia. Skúsenosti z projektu zároveň poukázali na viaceré oblasti, ktoré predstavujú dôležité poučenia pre ďalšie smerovanie.

V prípade rizika R7 sa potvrdilo, že je potrebné dôslednejšie sledovať kapacitné úzke miesta a včas identifikovať preťaženie členov tímu. Nedostatočné rozpoznanie tejto situácie viedlo k posunom viacerých výstupov. Ako dôležité odporúčanie sa preto ukazuje pravidelné preverovanie kapacít na úrovni pracovných balíkov, včasné zdieľanie dopadov medzi partnermi a vytváranie priestoru na pružné doplnenie personálnych kapacít podľa aktuálnej potreby.

Riziko R9 ukázalo, že aj pri využívaní spoločných komunikačných nástrojov môžu vznikať komunikačné nezrovnalosti, ktoré znižujú efektivitu spolupráce. Z tohto dôvodu sa ako dôležité poučenie javí potreba jasnejšie nastaviť komunikačné pravidlá, preferované nástroje a frekvenciu koordinačných stretnutí už v skorších fázach projektu. Vhodné je zároveň priebežne overovať, či zvolený komunikačný režim zodpovedá reálnym potrebám zapojených partnerov.

Pri riziku R15 sa ukázala potreba posilnenia internej kontroly kvality výstupov ešte pred ich oficiálnym odovzdaním. Odhalenie chýb až pri preberaní výstupu potvrdilo význam dôslednejšieho interného overovania podkladov. Do budúcnosti sa preto odporúča zaviesť systematickejšie kontrolné mechanizmy, ktoré prispejú k zníženiu chybovosti a k plynulejšiemu plneniu míľnikov.

Riziko R19 potvrdilo, že pri technologických riešeniach je potrebné priebežne preverovať ich vhodnosť aj počas realizácie projektu, nielen pri počiatočnom výbere. Zmena komerčného statusu komponentu „The Hive“ ukázala, že externé faktory môžu významne ovplyvniť realizáciu plánovaných aktivít. Do budúcnosti je preto vhodné klásť dôraz na dôsledné definovanie kritérií, priebežné overovanie udržateľnosti zvolených riešení a pripravenosť na alternatívne technologické varianty.

V prípade rizika R25 sa potvrdilo, že aj predvídateľné obdobia, ako sú letné dovolenky, môžu výrazne ovplyvniť koordináciu tímu. Za dôležité odporúčanie preto možno považovať včasné plánovanie neprítomností, transparentné zdieľanie týchto informácií a prispôsobenie koordinačného režimu obdobiam zníženej dostupnosti členov tímu.

Odporúčania pre ďalšie odborné smerovanie riešenia

Popri organizačných a projektových poučeniach projekt identifikoval aj kľúčové oblasti pre ďalší rozvoj navrhnutého SOCaaS riešenia.

Medzi kľúčové smery ďalšieho rozvoja riešenia patrí prehlbovanie integrácie medzi jednotlivými vrstvami architektúry, najmä medzi SIEM, SOAR, CTI a incident management komponentmi. Práve úroveň ich prepojenia sa ukazuje ako jeden z rozhodujúcich faktorov celkovej efektívnosti riešenia, a to najmä z pohľadu rýchlosti spracovania incidentov, obohacovania udalostí o kontext a konzistentnosti reakčných postupov. Ďalšou významnou oblasťou je spracovanie procesnej stránky a personálneho zabezpečenia prevádzky SOC.

Skúsenosti z projektu ukázali, že technologická architektúra musí byť sprevádzaná aj jasne definovanými rolami, zodpovednosťami, komunikačnými väzbami a kapacitným plánovaním tímu. Bez primeraného procesného a organizačného rámca nie je možné dlhodobo zabezpečiť stabilnú a efektívnu prevádzku navrhnutého riešenia.

Za otvorenú technickú výzvu, na ktorú je potrebné sa bližšie zamerať, považujeme rozpracovanie spôsobu oddelenia dát, prístupových práv, incidentných workflow a prevádzkových kontextov medzi jednotlivými tenantmi tak, aby bol zachovaný nielen funkčný, ale aj bezpečnostný a prevádzkový aspekt poskytovania služby. Dôležitým smerom ďalšieho rozvoja riešenia je aj vyššia miera automatizácie. Projekt potvrdil prínos automatizovaných integračných a reakčných mechanizmov, pričom ďalší rozvoj by sa mal orientovať najmä na rozšírenie playbookov, automatizáciu obohacovania incidentov a znižovanie podielu manuálnych krokov pri opakovateľných činnostiach SOC analytikov.

Ďalšou identifikovanou oblasťou je rozšírenie testovania na väčší rozsah scenárov a realistickejšie prevádzkové podmienky. Ďalšie overovanie by malo smerovať nielen na funkčnosť jednotlivých komponentov, ale aj na robustnosť integračných tokov, reakciu na komplexnejšie incidentné situácie a stabilitu riešenia pri vyššom objeme dát a udalostí. V neposlednom rade, perspektívnou oblasťou ďalšieho smerovania zostáva aj využitie metód strojového učenia pri detekcii anomálií a podpore rozhodovania v SOC prostredí. Ďalší rozvoj v tejto oblasti by mohol prispieť k presnejšej identifikácii vybraných typov incidentov, lepšiemu triedeniu udalostí a efektívnejšiemu spracovaniu rozsiahlejších dátových tokov.

Celkovo možno konštatovať, že projekt priniesol dôležité poznatky nielen v oblasti riadenia kapacít, komunikácie, kontroly výstupov a technologického rozhodovania, ale aj pri návrhu a overovaní architektúry multitenantného SOCaaS riešenia. Získané skúsenosti predstavujú vhodný základ pre efektívnejšie nastavenie podobných projektov aj pre ďalší odborný rozvoj navrhnutého riešenia.