PROJEKT

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

V24 aktualizovaný logický rámec projektu

KPB8 – Proj. dokumentácia

typ – dokumentácia

mesiac odovzdania – M3

Obsah

1. AKTUALIZOVANÝ LOGICKÝ RÁMEC

Využitie metódy logického rámca pre podporu vysokej kvality procesov projektového manažmentu aplikovaného v danom projekte. Na logický rámec projektu je nadviazaná hierarchická štruktúra prepájajúca najvrchnejší pohľad na projekt s komponentami produktu projektu a z nich vyplývajúcimi balíkmi práce (WP).

Tabuľka 1 Logický rámec

Opis projektu	Indikátory	Zdroje verifikácie	Predpoklady
Hlavným cieľom projektu INNOSOC je 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.	• dosiahnutie špecifických cieľov	• dokumentácia popisujúca technologické riešenie • modely (architektúra riešenia, ArchiMate modely, UML modely) • funkčný webový portál s príspevkami • publikačné výstupy • záverečná správa	-
Špecifické ciele SG1: Návrh technologického riešenia pre prevádzkovanie služby SOC s využitím virtualizovaných riešení spracovanom až na úroveň TRL3.	• MTTR* • HA • priemerná doba odozvy systému • stupeň automatizácie • nákladovosť • efektívnosť riešenia	• modely (architektúra riešenia, ArchiMate modely, UML modely) • dokumentácia popisujúca mechanizmy (automatizácia, monitoring, zálohovanie...) • dokumentácia návrhu systému	• tvorba dokumentu prepájajúceho relevantné výstupy projektu pre každú zainteresovanú stranu • aplikovateľnosť riešenia • naplnenie hlavných deklarovaných požiadaviek na výsledné riešenie
SG2: Návrh inteligentného systému pre monitoring technologických prostriedkov a služieb.	• presnosť detekcie výpadkov • rýchlosť detekcie a reakcie • škálovateľnosť a efektivita využívania zdrojov (HW) • nastaviteľnosť alarmov • výkonnosť systému a aplikácií z hľadiska času	• vizualizácie, alerty, reportingy • dokumentácia popisujúca virtualizované riešenie	

**cieľové hodnoty pre jednotlivé KPI budú nastavené WP1; spôsob hodnotenia efektívnosti bude určený WP1*

Opis projektu	Indikátory	Zdroje verifikácie	Predpoklady
SG3: Návrh architektúry samotnej inovatívnej elastickej služby INNOSOC ako integrácie otvorených riešení a komponentov.	• čas zotrvania • MTTD • MTTR • MTTC • TTC • náklady riešenia • doba implementácie	• dokumentácia popisujúca roly potrebných špecialistov • dokumentácia popisujúca architektúru elastickej služby • modely (architektúra riešenia, ArchiMate modely, UML modely)	• tvorba dokumentu prepájajúceho relevantné výstupy projektu pre každú zainteresovanú stranu • aplikovateľnosť riešenia naplnenie hlavných deklarovaných požiadaviek na výsledné riešenie
SG4: Návrh vhodných algoritmov strojového učenia s aplikáciou hlbokých neurónových sietí pre riešenie úlohy detekcie a predikcie bezpečnostných a operačných anomálií.	• presnosť detekcie anomálií • miera falošne pozitívnych a falošne negatívnych výsledkov • počet identifikovaných bezpečnostných, operatívnych anomálií • rýchlosť detekcie • presnosť predikcie • náročnosť na zdroje	• algoritmy strojového učenia a ich popis	
SG5: Vytvorenie platformy pre zdieľanie nadobudnutých poznatkov v zmysle realizovaného projektu a zásad otvorenej vedy.	• počet aktívnych používateľov • počet zdieľaných dokumentov • spätná väzba (upresnené v texte zdôvodnenia projektu) • počet odborných článkov	• funkčný webový portál s príspevkami • publikačné výstupy • záznamy z realizovaných osvetových aktivít (prezenčné listiny, grafické výstupy...)	
Výsledky INNOSOC: • Návrh riešenia na úrovni TRL3 • Diseminácia poznatkov • Manažérske výstupy	• otvorenosť • multitenantnosť • výkonová flexibilita • typ riešenia – cloudová/kontajnerová služba • riešenie obsahujúce moduly pre detekciu a predikciu anomálii • využitie strojového učenia a neurónových sietí	• zoznam a spresnenie kritérií riešení • popis funkcionalít • dokumentácia navrhovaných procesov obsiahnutých v navrhovanom systéme • register rizík a opatrení	• zaradenie publikovaných článkov vo vedeckých databázach (WOS, Scopus) • pilotné overenie riešenia používateľmi • pozitívna spätná väzba od návštevníkov portálu • vyriešenie identifikovaných problémov

Opis projektu	Indikátory	Zdroje verifikácie	Predpoklady
Aktivity • Navrhnúť virt. riešenia • Navrhnúť SOCaaS služby • Navrhnúť ML algoritmov • Navrhnúť architektúru riešenia • Navrhnúť riešenia SOC • Vytvoriť publikačné výstupy • Realizovať osvetové aktivity • Vytvoriť proj. dokumentáciu • Vytvoriť záverečnú správu	-	-	• zistenie požiadaviek potenciálnych používateľov • definovanie kľúčových zručností potrebných na návrh riešenia • prístup k potrebným dátam • ochota ZS spolupracovať na činnostiach navrhnutých v projekte