I-02 Projektový zámer (projektovy_zamer)

naposledy upravil Peter Ďuriš

- 2026/02/19 16:02

Obsah

PROJEKTOVÝ ZÁMER

(Project brief)

Identifikovanie požiadaviek **na funkčnú časť riešenia**

Identifikácia projektu

Oprávnená osoba	Národná diaľničná spoločnosť
Názov projektu	Zavedenie nástrojov a služieb kybernetickej a informačnej bezpečnosti
Zodpovedná osoba	Ing. Juraj Németh, Ing. Marián Guoth
Realizátor projektu	Národná Diaľničná Spoločnosť

Schvaľovanie dokumentu/produktu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis
Vypracoval					
Overil					
Schválil					

Obsah

1 POPIS ZMIEN DOKUMENTU

1.1 História zmien (Kto dokument vypracoval)

Verzia	Dátum	Zmeny	Meno
0.1	13.11.2025	Prvý draft dokumentu	Peter Ďuriš

1.2 Detail revízií (Kto dokument revidoval / kontroloval – napr. QA)

Verzia	Dátum	Pozícia kontrolujúceho	Meno

1.3 Detail schválení (Kto dokument schválil – napr. štatutár úradu, RV, ...)

Verzia	Dátum	Pozícia odsúhlasujúceho	Meno

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

Účelom tohto projektového zámeru je definovať základný rámec projektu *„Zavedenie nástrojov a služieb kybernetickej a informačnej bezpečnosti“*, a to v súlade s požiadavkami vyhlášky MIRRI SR č. 401/2023 Z. z., metodikou riadenia projektov ISVS a procesom predbežného posúdenia investičných zámerov v MetaIS.

Dokument slúži ako prvotný, vysokoúrovňový opis zamýšľaného projektu a jeho cieľov, ktorý umožní:

- včas identifikovať potreby organizácie, problémové oblasti a očakávané prínosy projektu,
- preukázať opodstatnenosť projektu vo vzťahu k legislatívnym, bezpečnostným a prevádzkovým požiadavkám,
- určiť základný rozsah, vecné vymedzenie a hranice projektu,
- získať predbežné stanovisko MIRRI SR, ktoré je podkladom pre ďalšie fázy prípravy projektu a pre plánovanie rozpočtových zdrojov,
- zabezpečiť zhodu projektu s národnými koncepčnými dokumentmi v oblasti informatizácie, kybernetickej bezpečnosti a riadenia IT vo verejnej správe.

Projektový zámer zároveň definuje kľúčových stakeholderov, základné alternatívy riešenia, rámcové riziká a predpokladané prínosy projektu. Jeho úlohou je umožniť MIRRI SR včasné metodické usmernenie a overenie súladu projektu s princípmi:

- efektívnosti a hospodárnosti,
- bezpečnosti a odolnosti ISVS,
- digitálnej inklúzie a používateľskej orientácie,
- reuse a interoperability,
- proporcionality a udržateľnosti.

3. DEFINOVANIE PROJEKTU (PROJECT DEFINITION)

Predmetom projektu je zavedenie nástrojov a služieb kybernetickej a informačnej bezpečnosti. Týmto projektom rozširujeme pôvodnú primárnu ochranu prostredia (firewall, antivírus, DLP, MFA a iné nástroje) o rozšírený pohľad z hľadiska „multivendor strategy“. Tento pohľad je kľúčový, nakoľko eliminuje hrozbu z prípadnej chyby v konfigurácii konkrétneho bezpečnostného systému, systému ako takého, prípadne zlyhanie bezpečnostnej technológie. Kybernetická bezpečnosť je z pohľadu architektúry prierezovou oblasťou a teda realizuje sa skrz všetky vrstvy architektúry. Cieľom je získať centralizovaný pohľad a tak umožniť efektívne zvyšovanie bezpečnosti implementáciou bezpečnostných aktualizácii alebo implementovanie nastavení tzv. „best practices“ do jednotlivých častí IT a používaného software. IT podpora (interná alebo externá) by mala takto získať komplexný prehľad o systémoch a ich funkčných reláciách, ako aj aplikovateľné existujúce riziká. Jedná sa teda hlavne o kontinuálny audit bezpečnostných štandardov a odhaľovanie možných prebiehajúcich útokov.

Terajšia biznis vrstva architektúry IT nezodpovedá bezpečnostnému štandardu podľa vyhlášky o kybernetickej bezpečnosti alebo svetovému CIS framework podľa NIST. Samotným zavedením nových nástrojov a štandardov nedochádza k podstatným zmenám v rámci existujúcej infraštruktúry.

V rámci prípravy projektu prebehlo aj verejné pripomienkovanie od 24.11.2025 do 5.12.2025. V rámci pripomienkovania nebola doručená žiadna pripomienka. Oznámenie bolo zverejnené na stráne NDS - Cieľ 3.2: Zavádzanie bezpečných digitálnych produktov, služieb a inovácií https://ndsas.sk/spolocnost/projekty

3.1 Motivácia a rozsah projektu

3.1.1 Popis problému, ktorý má projekt odstrániť

Národná diaľničná spoločnosť (NDS) v súčasnosti prevádzkuje viacero kritických informačných systémov, bezpečnostných technológií a infraštruktúrnych komponentov, ktoré sú kľúčové pre správu diaľničnej siete a sú súčasťou prvkov kritickej infraštruktúry Slovenskej republiky. Bezpečnostné nástroje, procesy a dohľadové mechanizmy sú však **fragmentované, neprepojené a prevažne manuálne**, čo spôsobuje:

- obmedzenú schopnosť včas odhaliť kybernetický útok alebo anomáliu,
- vysokú záťaž pre IT pracovníkov pri manuálnom riešení incidentov,
- neprehľadnosť pri riadení rizík a zraniteľností,
- duplicitné alebo neúplné evidencie v Service Desk prostredí,
- nesúlad s legislatívnymi požiadavkami (ZoKB, NIS2).

Tento stav zvyšuje riziko vzniku kybernetických incidentov, predlžuje reakčný čas pri ich riešení a znižuje celkovú odolnosť organizácie voči hrozbám.

3.1.2 Dotknuté biznis procesy

Realizáciou projektu sa rieši modernizácia a podpora nasledujúcich biznis procesov, ktoré v súčasnosti trpia neefektívnosťou alebo nedostatočnou automatizáciou:

- Proces riadenia kybernetických incidentov – detekcia, eskalácia, riešenie a uzatváranie incidentov.
- Proces riadenia zmien a konfigurácií – evidencia zmien, koordinácia zásahov, správa konfiguračných položiek.
- Proces riadenia rizík a zraniteľností – identifikácia aktív, hodnotenie rizík, riešenie zraniteľností.
- Proces IT prevádzky a monitoringu infraštruktúry – dohľad nad sieťou, aplikáciami a dostupnosťou služieb.
- Proces správy požiadaviek používateľov (Service Desk) – evidencia požiadaviek, prideľovanie úloh, riešenie porúch.

Celkovo ide o **5 kľúčových procesných oblastí**, ktoré ovplyvňujú prevádzku kritickej infraštruktúry a interné fungovanie NDS.

3.1.3 Motivácia pre dosiahnutie budúceho stavu

Základnou motiváciou projektu je:

- výrazne zvýšiť **úroveň ochrany kritickej infraštruktúry**,
- skrátiť čas detekcie a reakcie na incidenty (MTTD/MTTR),
- odstrániť súčasnú reaktívnu bezpečnostnú prevádzku a nahradiť ju **proaktívnym, automatizovaným modelom**,
- splniť požiadavky štátnej legislatívy a EÚ regulácií,
- vytvoriť jednotné prostredie pre dohľad, reporting, evidenciu a auditné stopy,
- podporiť dlhodobú udržateľnosť bezpečnostnej prevádzky formou konzumácie služieb,
- odbremeniť interných zamestnancov od rutinných činností a umožniť im venovať sa strategickým aktivitám.

V konečnom dôsledku projekt minimalizuje riziko škôd a výpadkov, ktoré môžu mať významný ekonomický dopad aj dopad na dôveryhodnosť NDS ako prevádzkovateľa kritickej infraštruktúry.

3.1.4 Obmedzenia projektu

Pri realizácii projektu existujú nasledujúce obmedzenia:

- **Organizačné kapacity** – NDS má obmedzený počet IT a bezpečnostných pracovníkov, čo limituje rozsah internej implementácie.
- **Technické limity existujúcej infraštruktúry** – staršie systémy môžu mať nižšiu podporu integrácie do SIEM/NOC.
- **Zmluvné obmedzenia** – projekt musí byť v súlade s rámcovými zmluvami a nákupnými procesmi NDS.
- **Závislosť od externých služieb** – model Security as a Service vyžaduje vysokú kvalitu SLA a spoluprácu s partnerom.
- **Legislatívne povinnosti** – projekt musí zabezpečiť úplný súlad s NIS2 a ZoKB; ak sa nepodarí, vzniká riziko pokút.
- **Časové obmedzenia** – implementácia musí prebehnúť v súlade s termínmi transpozície NIS2 a interným harmonogramom obnovy bezpečnostných technológií.

3.1.5 Súlad projektu so strategickými dokumentami

Projekt prispieva k plneniu NKIVS 2025 a strategickej priority Kybernetická a informačná bezpečnosť v rámci cieľa Bezpečné informačné systémy verejnej správy (priame mapovanie). Projekt vo svojom rozsahu zabezpečí centralizovaný pohľad na zabezpečený perimeter a tak umožniť efektívne zvyšovanie bezpečnosti implementáciou

bezpečnostných aktualizácii alebo implementovanie nastavení tzv. „best practices“ do jednotlivých častí IT a používaného software.

Rovnako je projekt v súlade s novou stratégiou kybernetickej bezpečnosti na roky 2026 až 2030, ktorá bola schválená vládou 4.2.2026, pričom prispieva k napleneniu nasledovných cieľov:

- Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb
- Cieľ 2.2: Efektívne zavádzanie bezpečnostných technológií a procesov
- Cieľ 3.2: Zavádzanie bezpečných digitálnych produktov, služieb a inovácií

3.1.6 Rozsah projektu

Prostredie je obsiahle s priamym dopadom na prevádzku. Súčasné prostredie obsahuje nasledovné technológie: Kaspersky EDR a XDR, Fortinet Firewally, Novicom, Thales MFA, MS AD, Cloud apps, 1200 používateľov, 10000 zariadení (IT, IoT, OT).

Existujúce prostredie je heterogénne, pozostávajúce z maximálne 10000 zariadení.

- Jednotlivé funkčné celky sú izolované.
- Najväčšia centralizovaná časť je Microsoft Active Directory, kde je 1200 aktívnych účtov.
- využívame alebo plánujeme využívať Microsoft 365 služby, ako aj čiastočne Azure, prípadne AWS prostredie
- Existujúce technológie nejdeme vymieňať, ale dopĺňať, pričom riešenia musia byť kompatibilné s existujúcim stavom.

Existujúce nástroje primárnej ochrany postrádajú centrálny nástroj pre korelovanie jednotlivých záznamov a udalostí. Existujúca primárna ochrana je postavená na predpoklade, že je plne funkčná a dostatočne bezpečná. Pokiaľ zlyhá primárna ochrana v ľubovoľnom bode, čase, alebo jednoducho nezachytí „vírus, malware, ransomware, alebo priamo útočníka“, nie sme schopní efektívne a rýchlo zistiť takéto zlyhanie, alebo konfiguračná chybu. Preto považujeme za nevyhnutné mať nezávislé hodnotenie funkčnosti tejto primárnej technológie.

- Zlyhanie patch management procesu = vulnerability management
- Zlyhanie firewallu a prepustenie škodlivej komunikácie = sondy v sieti
- Zlyhanie antivíru = nezávislé EDR
- Zlyhanie IDP a MFA = nezávislý SIEM s identifikáciou napr. lateral movement
- A iné príklady.

Existujúca databáza asetov nie je určená primárne na vyhodnocovanie bezpečnosti a teda v nej chýbajú informácie pre efektívne vyhodnocovanie bezpečnostných rizík a súvislostí napr. Critical path mapping, prípadne effective permission, alebo nezávislé vyhodnocovanie zhody so štandardami napr. CIS framework.

Všetky nástroje sa budú implementovať po jednotlivých celkoch a úsekoch. Pri ponuke treba zohľadniť možnosť postupného nákupu licencií na celkový počet zariadení alebo užívateľov. Cieľom je implementovať všetky navrhované súčasti v čo najkratšej dobe. Celkovú realizáciu obstarávame na 4 roky, pričom objednávateľ sa nezaväzuje licenčne pokryť celé prostredie jednotlivými technológiami. Zákazník si vyhradzuje právo nakupovať licencie po jednotkách až desiatkach podľa potreby a aktuálneho štádia projektu. Všetky nástroje sa obstarávajú vrátane Inštalácie a konfigurácie s následnou správou.

Exposure and Risk management

V súčasnom dynamickom a čoraz sofistikovanejšom digitálnom prostredí čelia organizácie neustále sa vyvíjajúcim hrozbám, ktoré môžu ohroziť ich bezpečnosť, integritu dát a prevádzkovú kontinuitu. Kybernetické útoky, ako sú sofistikované prieniky, úniky údajov, ransomvérové útoky či zneužitie zraniteľností v infraštruktúre, predstavujú významné riziko pre podniky všetkých veľkostí a odvetví. V tomto kontexte je nasadenie nástrojov pre správu expozície a rizík (Exposure a Risk Management) nielen strategickou nevyhnutnosťou, ale aj kľúčovým predpokladom pre zachovanie dôvery zákazníkov, ochranu reputácie a zabezpečenie súladu s regulačnými požiadavkami.

Nástroje pre Exposure a Risk Management umožňujú organizáciám systematicky identifikovať, monitorovať a zmierňovať potenciálne hrozby v ich internom aj externom prostredí. Tieto riešenia poskytujú komplexný pohľad na zraniteľnosti v infraštruktúre, aplikáciách a procesoch, čím umožňujú proaktívne riadenie rizík ešte predtým, ako sa stanú kritickými incidentmi. Vďaka nim môžu organizácie efektívne reagovať na nové hrozby, minimalizovať dopady narušení a optimalizovať svoje bezpečnostné stratégie. Nasadenie týchto nástrojov zároveň zvyšuje odolnosť voči kybernetickým hrozbám a podporuje dlhodobú udržateľnosť podnikania.

V nasledujúcich kapitolách budú podrobne rozpracované jednotlivé podporné technológie, ako sú Internal Attack Surface, External Attack Surface, Threat Intelligence, Digital Risk Protection, Cloud Posture, Threat Third Party, SOAR a SIEM. Tieto technológie spoločne vytvárajú robustný ekosystém pre správu bezpečnostných rizík, ktorý je prispôsobený špecifickým potrebám organizácie a aktuálnym trendom v oblasti kybernetickej bezpečnosti.

Riešenie pre všetky podkapitoly state musí byť dodané ako jednotný funkčný celok. Riešenie musí byť plne integrované a podporované jedným výrobcom alebo v rámci jedného servisného kontraktu.

Internal Attack Surface Management

Internal Attack Surface Management je kľúčovým prvkom pre zabezpečenie organizácie pred hrozbami pochádzajúcimi zvnútra jej infraštruktúry. Tento proces zahŕňa identifikáciu, monitorovanie a zmierňovanie zraniteľností v interných systémoch, sieťach a aplikáciách, ktoré by mohli byť zneužité útočníkmi. Efektívna správa umožňuje organizáciám minimalizovať riziká spojené s internými hrozbami, ako sú chyby konfigurácie, zastarané systémy či neoprávnený prístup. Základným predpokladom je mať zmapované hrozby z interného prostredia pomocou ďalej upresnených nástrojov, ktorých výstup sa stretáva v jednej centrálnej konzole. V tejto konzole je následne možné priorizovať hrozby a sústrediť sa na najkritickejšie zraniteľnosti z pohľadu pravdepodobnosti zneužitia ako aj dopadu.

Vulnerability management

Správa zraniteľností (Vulnerability Management) je systematický proces identifikácie, hodnotenia a opravy zraniteľností v interných systémoch a aplikáciách. Tento proces zahŕňa pravidelné skenovanie infraštruktúry, analýzu potenciálnych slabín a implementáciu opráv alebo zmierňujúcich opatrení. Správa zraniteľností zaisťuje, že organizácia je schopná rýchlo reagovať na novoobjavené hrozby a minimalizovať riziko ich zneužitia, čím posilňuje celkovú bezpečnostnú pozíciu. Základným predpokladom je mať potvrdené hrozby (ciže identifikované a overené na systéme – ako napríklad závislost RPM balíčkov na Linuxe). Systém musí vedieť identifikovať a skenovať všetky zariadenia v sieti, nesmie sa spoliehať na nainštalovaného agenta. Okrem bezpečnostných zraniteľností systém musí reportovať aj zhody s požadovanými nastaveniami (compliance) s preddefinovanými world wide štandardmi (CIS, PCI DSS, HIPAA, GDPR, atď). Cieľom poznať zraniteľnosti aj tzv. „black box“ riešení, alebo komponentov siete, ktoré nemajú operačný systém a možnosť inštalácie agenta.

Dynamic Application Security Testing

Dynamické testovanie bezpečnosti aplikácií (Dynamic Application Security Testing, DAST) sa zameriava na identifikáciu zraniteľností v aplikáciách za behu, simulujúc útoky z pohľadu externého útočníka. Tento prístup umožňuje odhaliť slabiny, ako sú chyby v správe relácií, injekčné útoky či nedostatočná autentifikácia. DAST je nevyhnutné pre zabezpečenie interných aplikácií, ktoré sú často kritickým bodom pre prieniky do infraštruktúry. Podmienkou je skenovanie aplikácií pre OWASP top 25.

Cloud Posture

Správa bezpečnostného stavu cloudu (Cloud Posture) sa sústreďuje na monitorovanie a zabezpečenie cloudových prostredí, ktoré sa stali neoddeliteľnou súčasťou modernej IT infraštruktúry. Tento proces zahŕňa hodnotenie konfigurácií cloudových služieb, identifikáciu nesprávnych nastavení a zabezpečenie súladu s bezpečnostnými štandardmi. Správa cloudového postoja chráni organizáciu pred rizikami spojenými s neautorizovaným prístupom, únikmi dát či zneužitím cloudových zdrojov. Nástroj monitoruje oprávnenia v rámci Cloud prostredia a upozorňuje na ich opodstatnenosť, prípadne aktuálnosť, externé prístupy (CIAM). Okrem complinace, vulnerability, CIAM nástroj musí vyhodnocovať aj IaC (Infrastructure as Code) a umožniť automatické nápravy. Celkový pohľad na prípadné nedostatky musí byť graficky interpretovaný pomocou napr. „Heat Map“ a „Critical Attack Path“.

External Attack Surface Management

External Attack Surface Management je zameraná na identifikáciu a ochranu aktív organizácie, ktoré sú vystavené vonkajšiemu prostrediu, ako sú webové stránky, verejné servery či API. Tento proces umožňuje organizáciám proaktívne odhaľovať a zmierňovať riziká spojené s externými hrozbami, čím znižujú pravdepodobnosť úspešných kybernetických útokov. Na rozdiel od Internal Attack Surface tento pohľad zahŕňa end-to-end bezpečnostné nástroje a ich nastavenie. Okrem testovania „otvorených portov“ je potrebné aj prieskum o prípadné uniknuté dáta alebo včasné odhalenie plánovaných útokov na spoločnosť alebo jej kľúčové osoby a to aj nepriamo prostredníctvom preverenia Supply Chain hrozieb.

Digital Risk protection

Ochrana digitálnych rizík (Digital Risk Protection) sa zameriava na monitorovanie a zmierňovanie hrozieb v digitálnom priestore, ako sú úniky údajov, falošné domény či zneužitie značky. Tento proces zahŕňa analýzu dark webu, sociálnych médií a iných externých zdrojov, aby sa identifikovali potenciálne hrozby ešte pred ich eskaláciou. Digitálna ochrana rizík pomáha chrániť reputáciu a dôveru zákazníkov. Súčasťou je monitorovanie spoofingu alebo phishingu.

Third Party Scanning

Skenovanie tretích strán (Third Party Scanning) je zamerané na hodnotenie bezpečnosti externých partnerov, dodávateľov a ich systémov, ktoré sú prepojené s infraštruktúrou organizácie. Tento proces identifikuje zraniteľnosti v dodávateľskom reťazci, ktoré by mohli byť zneužité na prienik do organizácie. Skenovanie tretích strán je kľúčové pre zabezpečenie celistvosti ekosystému organizácie, vyžadované aj podľa zákona a ISO.

Tactical Intelligence

Taktická inteligencia (Tactical Intelligence) poskytuje organizáciám aktuálne a konkrétne informácie o hrozbách, ktoré môžu ovplyvniť ich externý povrch útoku. Tieto informácie zahŕňajú údaje o nových exploitoch, útočných technikách či zraniteľnostiach. Taktická inteligencia umožňuje rýchlu reakciu na vznikajúce hrozby a zlepšuje efektivitu bezpečnostných opatrení.

Operational Intelligence

Operačná inteligencia (Operational Intelligence) sa zameriava na zhromažďovanie a analýzu dát z externého prostredia v reálnom čase, aby sa zabezpečila kontinuálna ochrana. Tento proces integruje informácie z viacerých zdrojov a poskytuje organizáciám prehľad o aktuálnom stave ich bezpečnosti. Operačná inteligencia podporuje rýchle rozhodovanie a efektívne riadenie incidentov.

Exposure Management

Správa expozície (Exposure Management) je komplexný proces, ktorý zahŕňa hodnotenie, prioritizáciu a zmierňovanie rizík spojených s interným aj externým povrchom útoku. Tento proces zaisťuje, že organizácia dokáže efektívne alokovať zdroje na riešenie najkritickejších hrozieb, čím maximalizuje svoju odolnosť voči kybernetickým útokom.

Assessment

Hodnotenie (Assessment) je prvým krokom v správe expozície, ktorý zahŕňa identifikáciu a analýzu potenciálnych zraniteľností a hrozieb v celom IT prostredí. Tento proces poskytuje detailný prehľad o slabých miestach a umožňuje organizáciám pochopiť rozsah svojej expozície voči rizikám.

Prioritization

Prioritizácia (Prioritization) umožňuje organizáciám triediť identifikované riziká podľa ich závažnosti a potenciálneho dopadu. Tento proces zohľadňuje faktory ako pravdepodobnosť zneužitia, kritickosť postihnutých systémov a možné následky. Prioritizácia zaisťuje efektívne využitie zdrojov na riešenie najnaliehavejších hrozieb.

Remediation (SOAR)

Oprava (Remediation) prostredníctvom nástrojov SOAR (Security Orchestration, Automation, and Response) umožňuje automatizáciu a orchestráciu reakcií na bezpečnostné incidenty. SOAR integruje rôzne bezpečnostné nástroje a procesy, čím urýchľuje reakciu na hrozby, znižuje manuálnu prácu a zvyšuje efektivitu zmierňovania rizík. SOAR môže zabezpečovať

Risk Management (SIEM)

Správa rizík (Risk Management) prostredníctvom systémov SIEM (Security Information and Event Management) poskytuje organizáciám centralizovanú platformu na monitorovanie, analýzu a reakciu na bezpečnostné udalosti v reálnom čase. SIEM zaisťuje komplexný prehľad o bezpečnostnom stave organizácie a podporuje proaktívne riadenie rizík. SIEM by mal zbierať logy z infraštruktúrnych serverov, bezpečnostných technológii, aplikácii, SaaS a cloud zdrojov, z vlastných nástrojov typu monitoring siete a koncových stanic, DFIR nástroje. Zásadná je prepojitelnosť primárne s vulnerability management nástrojom a threat intelligence, kde SIEM by mal konzumovat IoC (indicator of compromise). Úzka integrácia so SOAR nástrojom je kritická pre efektívne obohacovanie dát, ako aj reakciu na incidenty.

Service Desk

Predmetom súťaže je dodávka a implementácia diela – SW riešenia „Service Desk“ a následné služby technickej podpory. Samotný nástroj Service je určený ako primárna komunikačná platforma medzi IT operations, SOC a jednotlivými stakeholders (dodávatelia, zamestnanci, management. Tento nástroj má slúžiť primárne na interaktívnu komunikáciu medzi zúčastnenými stranami a má tvoriť dokumentárnu funkciu požiadaviek a hlásených incidentov. Nástroj však musí byť pripravený aj na integráciu automatického zaznamenávania z jednotlivých nástrojov popísaných v tomto dokumente, existujúceho monitoringu prostredia a podobne.

Riešenie pre všetky podkapitoly state musí byť dodané ako jednotný funkčný celok. Riešenie musí byť plne integrované a podporované jedným výrobcom alebo v rámci jedného servisného kontraktu.

Incident mgmt

Správa incidentov (Incident Management) sa zameriava na rýchle obnovenie normálnej prevádzky služieb po výskyte incidentu, ako sú výpadky systémov alebo poruchy aplikácií. Zahŕňa zaznamenávanie, kategorizáciu, prioritizáciu a riešenie incidentov, ako aj komunikáciu s používateľmi. Cieľom je minimalizovať dopad na podnikové procesy a zabezpečiť kontinuitu služieb. Je primárnym zdrojom pre vyhodnocovanie SLA.

Change mgmt

Správa zmien (Change Management) umožňuje plánovanie, schvaľovanie a implementáciu zmien v IT prostredí, ako sú aktualizácie softvéru alebo zmeny konfigurácie. Tento proces zahŕňa hodnotenie rizík, koordináciu zmien a dokumentáciu, aby sa minimalizovali potenciálne narušenia a zabezpečil súlad s podnikovými politikami. Tento modul slúži ako primárny podklad pre Change Advisory Board

Problem mgmt

Správa problémov (Problem Management) sa sústreďuje na identifikáciu a odstraňovanie základných príčin opakujúcich sa incidentov. Zahŕňa analýzu problémov, návrh preventívnych opatrení a vytváranie známych chýb (Known Error Database), aby sa predišlo budúcim narušeniam a zlepšila kvalita služieb.

Request Manahgement

Správa požiadaviek (Request Management) podporuje spracovanie požiadaviek používateľov, ako sú žiadosti o nové vybavenie, prístupy alebo informácie. Tento proces zahŕňa samoobslužné portály, automatizované schvaľovacie postupy a sledovanie stavu požiadaviek, čím sa zvyšuje efektivita a používateľská spokojnosť. Musí obsahovať tvorbu vlastných formulárov a následnú automatizáciu.

Configuration management

Správa konfigurácií (Configuration Management) zabezpečuje evidenciu a správu informácií o IT aktívach a ich konfiguráciách v Configuration Management Database (CMDB). Tento proces umožňuje prehľad o vzťahoch medzi aktívami, podporuje plánovanie zmien a uľahčuje rýchlu identifikáciu príčin incidentov.

Risk Management

Správa rizík (Risk Management) v Service Desk nástroji identifikuje, hodnotí a zmierňuje riziká spojené s IT službami a zmenami. Zahŕňa analýzu potenciálnych dopadov zmien, monitorovanie bezpečnostných hrozieb a implementáciu opatrení na minimalizáciu rizík, čím sa zvyšuje stabilita a bezpečnosť IT prostredia. Jeho primárny účel je evidencia rizík a tzv. Risk Acceptance protokolov poukazujúcich na prípadné zlyhania, na ktoré nie je možné uplatniť SLA.

Service Catalog

Katalóg služieb (Service Catalog) poskytuje používateľom prehľad dostupných IT služieb a ich popisov, ako sú požiadavky na prístup, softvér alebo hardvér. Umožňuje samoobslužné objednávanie služieb, zjednodušuje komunikáciu a zvyšuje transparentnosť poskytovaných služieb.

SLA, reporting

Správa dohôd o úrovni služieb (SLA) a reportovanie zahŕňajú definovanie, monitorovanie a hodnotenie úrovne poskytovaných služieb v súlade s dohodnutými SLA. Nástroje ponúkajú automatizované sledovanie metrík, generovanie prehľadov a analýz, ktoré podporujú rozhodovanie, zlepšovanie služieb a preukazovanie súladu s požiadavkami.

Nástroj pre NOC (Network Operation Center)

V záujme viditeľnosti toku dát a potenciálneho nebezpečia prepusteného firewallom je potrebné zabezpečiť viditeľnosť a analýzu dátových tokov na sieti v dvoch lokalitách. (2x SFP+ 10Gbps na každej). Realizácia by mala byť formou inštalácie HW NW sondy do siete na Core switch formou zrkadlenia traffic. Zbytok segmentov vyžaduje iba čiastočný monitoring nezávislým systémom prioritne zameraný na IDS napojeným do SIEM. Hlavné segmenty však musia mať pokročilejší behaviorálny monitoring na odhaľovanie anomálií, sledovanie svojpomocne definovaných paketov prostredníctvom YARA a STIX/TAXII definícií. Okrem sledovania anomálií a potenciálnych hrozieb musí byť systém schopný vyhodnocovať výkonnosť aplikácií a merať odozvy systémov na aplikačnej úrovni.

Riešenie pre všetky podkapitoly state musí byť dodané ako jednotný funkčný celok. Riešenie musí byť plne integrované a podporované jedným výrobcom alebo v rámci jedného servisného kontraktu.

SOC services

Služby Security Operations Center (SOC) predstavujú pilier pre zabezpečenie komplexnej ochrany organizácie pred kybernetickými hrozbami. SOC služby poskytujú nepretržité monitorovanie, detekciu, analýzu a reakciu na bezpečnostné incidenty v reálnom čase, čím zaisťujú ochranu kritických systémov, dát a infraštruktúry. Tieto služby kombinujú pokročilé technológie, ako sú SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), Exposure Management a analytické nástroje, s odbornými znalosťami bezpečnostných analytikov, aby efektívne identifikovali a zmierňovali hrozby. V rámci definície SOC služieb bude vypracovaný zoznam kompetencii medzi security operations a IT operations. Security operation prevezme do správy nástroje implementované v tomto projekte, ako aj existujúce bezpečnostné technológie. Konkrétne požiadavky budú doplnené v prílohe.

SOC team by mal byt rozdelený na viacero úrovní, pričom jednotlivé celky by mali zabezpečovať:

- Monitorovanie a detekcia: Neustále sledovanie IT prostredia (siete, aplikácií, koncových bodov) na identifikáciu podozrivých aktivít a anomálií.
- Analýza a reakcia na incidenty: Rýchla analýza bezpečnostných udalostí a koordinovaná reakcia na zmiernenie dopadov, vrátane forenznej analýzy a nápravy.
- Správa hrozieb: Využitie dát z Threat Intelligence na proaktívne odhaľovanie nových hrozieb a zraniteľností.
- Automatizácia a orchestrácia: Implementácia SOAR nástrojov na automatizáciu rutinných úloh a urýchlenie reakcií na incidenty. Ako aj integrácia systémov do SIEM
- Súlad a reportovanie: Zabezpečenie súladu s regulačnými požiadavkami (napr. GDPR, ISO 27001) a poskytovanie pravidelných správ o bezpečnostnom stave.
- Incident response: Forenzná analýza eskalovaných hrozieb spojená Threat Hunting službami s cieľom objaviť infiltráciu nebezpečného kódu alebo útočníka, s následným odstránením týchto hrozieb a zistenie prieniku do systémov spolu s proaktívnym odporúčaním na odstránenie cesty útoku.

Dôležité súčasti SOC sú tactical a operational Intelligence pre včasné varovanie a Incident Response pre prípad odhalenia prebiehajúceho útoku a následné zmiernenie škôd, právne poradenstvo prípadne služby vyjednávača. Incident Response služby okrem izolovania problému riadia aj obnovenie a rozchodenie systému pri jeho celkovom zlyhaní (napr. katastrofický ransomware útok). V prípade nevyužitia týchto služieb počas roka je možné expertízne služby čerpať aj na iné účely typu Penetration testing a Red Teaming alebo bezpečnostný audit.

3.2 Zainteresované strany/Stakeholderi

Zainteresované strany v rámci projektu sú všetci interní zamestnanci, externí dodávatelia a užívatelia služieb a produktov NDS. Projekt zabezpečuje stabilitu infraštruktúry s možnosťou rýchlejšie zistiť škodlivú činnosť a predchádzať potenciálnym následkom. Jedná sa primárne o doplnkový monitoring od nezávislých výrobcov primárnej IT bezpečnostnej technológie, čo značí, že vieme kontrolovať aj prípadné zlyhanie konkrétneho výrobcu.

Primárni stakeholderi sú:

- **IT Operation:** Security Operation Center (outsoursovaný SOC) má za úlohu upozorňovať IT operation proaktívne na odstraňovanie bezpečnostných rizík
- **MKB:** manažér Kybernetickej bezpečnosti bude mať k dispozícii takmer okamžitý prehľad o vzniknutých potenciálnych hrozbách a bezpečnostný prehľad o infraštruktúre, čo mu umožní lepšie predvídať a plánovať kroky pre zachovanie kontinuity prevádzky.
- **Štatutár:** ako priamo zodpovedný za prevádzku kritickej infraštruktúry bude mať jasný prehľad podložený faktami o potrebe investícií do konkrétnych oblastí. Zároveň má alokovaný externý tím pre riešenie neočakávaných incidentov.

- **Ekonomický riaditeľ a HR:** predvídateľný náklad na prevádzku bezpečnosti bez potreby školenia interného personálu a zvyšovania kapacít.
- **Užívatelia služieb a produktov NDS:** prevádzka bez neočakávaných výpadkov, prípadne minimalizovanie času obnovy prevádzky na minimum z dôvodu bezpečnostných incidentov
- **CSIRT a NBU:** jednoznačná identifikácia podozrivých útokov a odhaľovanie priemyselnej špionáže, ako aj organizovaných útokov umožňuje efektívne hlásenie podozrivých akcii na vyšší orgán pre spracovanie na národnej úrovni.

3.3 Ciele projektu

Predmetom projektu je zavedenie nástrojov a služieb kybernetickej a informačnej bezpečnosti. Týmto projektom rozširujeme pôvodnú primárnu ochranu prostredia (firewall, antivírus, DLP, MFA a iné nástroje) o rozšírený pohľad z hľadiska „multivendor strategy“. Tento pohľad je kľúčový, nakoľko eliminuje hrozbu z prípadnej chyby v konfigurácii konkrétneho bezpečnostného systému, systému ako takého, prípadne zlyhanie bezpečnostnej technológie. Kybernetická bezpečnosť je z pohľadu architektúry prierezovou oblasťou a teda realizuje sa skrz všetky vrstvy architektúry. Cieľom je získať centralizovaný pohľad a tak umožniť efektívne zvyšovanie bezpečnosti implementáciou bezpečnostných aktualizácii alebo implementovanie nastavení tzv. „best practices“ do jednotlivých častí IT a používaného software. IT podpora (interná alebo externá) by mala takto získať komplexný prehľad o systémoch a ich funkčných reláciách, ako aj aplikovateľné existujúce riziká. Jedná sa teda hlavne o kontinuálny audit bezpečnostných štandardov a odhaľovanie možných prebiehajúcich útokov.

Merateľné ukazovatele/KPI

ID	CIEĽ	NÁZOV MERATEĽNÉHO UKAZOVATEĽA A VÝKONNOSTNÉHO UKAZOVATEĽA (KPI)	POPIS UKAZOVATEĽA	MERNÁ JEDNOTKA (v čom sa meria ukazovateľ)	AS-IS MERATEĽNÉ VÝKONNOSTNÉ HODNTOY (aktuálne hodnoty)	TO-BE MERATEĽNÉ VÝKONNOSTNÉ HODNTOY (cieľové hodnoty projektu)	SPÔSOB MERANIA/ OVERENIA PO NASADENÍ (overenie naplnenie cieľa)	POZNÁMKA
1	Zrýchlenie detekcie bezpečnostných incidentov	**MTTD – Mean Time To Detect**	Priemerný čas od vzniku bezpečnostného incidentu po jeho detekciu bezpečnostnými nástrojmi alebo SOC	minúty	Nie je systematicky merané	≤ **15 min** pre kritické incidenty	Porovnanie časových značiek incidentov v SIEM a SOC reportoch	Vzťahuje sa na incidenty klasifikované ako kritické
2	Zrýchlenie reakcie na bezpečnostné incidenty	**MTTR – Mean Time To Respond**	Priemerný čas od detekcie incidentu po začatie reakčných opatrení	minúty	Nie je systematicky merané	≤ **60 min** pre kritické incidenty	SOC/SOAR reporty – čas otvorenia incidentu a spustenia reakcie	Viazané na SLA SOC služieb
3	Zvýšenie viditeľnosti bezpečnostných udalostí	**Pokrytie logovaním kritických systémov**	Podiel kritických systémov a zariadení poskytujúcich logy do centrálneho SIEM	%	Čiastočné, nejednotné	≥ **95 %** kritických systémov	Porovnanie CMDB / inventára aktív so SIEM inventárom log zdrojov	Kritické systémy definované v architektúre
4	Zvýšenie kvality bezpečnostných dát	**Kvalita bezpečnostných logov**	Podiel logov obsahujúcich povinné atribúty (čas,	%	Neštandardizovaná kvalita	≥ **90 %** logov spĺňa požiadavky	Automatizované kontroly kvality logov v SIEM	Požiadavky vychádzajú z CIS a ZoKB

			zdroj, cieľ, typ udalosti)					
5	Zabezpečenie kontinuálnej dostupnosti SOC služieb	**Dostupnosť SOC služieb**	Percentuálna dostupnosť monitoringu a reakčných služieb SOC	%	Nie je formálne definované	≥ **99,9 %**	SLA reporty poskytovateľa SOC	Definované v zmluve o SOC službách

3.4 Špecifikácia potrieb koncového používateľa

Tento projekt nie je zameraný na vývoj alebo rozvoj ISVS/s elektronickými službami , ktoré majú grafické alebo iné používateľské rozhranie, pričom nie je jeho realizácia určená pre občanov/podnikateľov (alebo aj pracovníkov verejnej správy pracujúcich s agendovým systémom).

3.5 Vyhodnotenie rizík a závislostí

Je súčasťou prílohy tohto dokumentu - P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI_Projekt_SOC_NDS

3.6 Detailný opis rozpočtu projektu a jeho prínosov

V tejto časti sú popísané náklady a prínosy navrhovaného riešenia

3.6.1 Sumarizácia nákladov

Celkové náklady projektu rozvoja boli stanovené v 10 ročnom horizonte metodikou prieskumu trhu a následnej aproximácie nákladov. Prieskum trhu bol zameraný na zistenie nákladov na zabezpečenie služieb Zavedenie nástrojov a služieb kybernetickej a informačnej bezpečnosti , pričom tieto sa skladali z nasledovných položiek:

- Exposure and Risk management
- Service Desk
- Nástroj pre NOC (Network Operation Center)
- SOC SERVICES

Pričom boli naceňované iniciačné náklady a následné poskytovanie služieb KB. Tieto služby boli necenené na 4 roky. Následné roky boli ohodnotené 75% hodnotou z prevádzkových nákladov aj vzhľadom na fakt, že je predpoklad znižovania cien poskytovaných služieb. Všetky hodnoty sú uvedené bez DPH.

Sumarizácia nákladov sa nachádza v nasledujúcej tabuľke:

TO BE - AS IS (€, SUM)				
			Spolu	SOC
Náklady s DPH			**9 772 470 €**	**9 772 470 €**
	Všeobecný materiál		- €	- €
	IT - CAPEX		4 751 928 €	4 751 928 €
		Aplikácie	- €	- €
		SW	*4 751 928 €*	*4 751 928 €*
		HW	- €	- €
	IT - OPEX		5 020 542 €	5 020 542 €
		Aplikácie	- €	- €
		SW	*5 020 542 €*	*5 020 542 €*
		HW	- €	- €
	Riadenie projektu		- €	- €
	Výstupné náklady		- €	- €
Prínosy			**9 500 000 €**	**9 500 000 €**

3.6.2 Popis a kvantifikácia prínosov projektu

V rámci ekonomickej analýzy je kladený dôraz predovšetkým na definovanie prínosov navrhovaného projektu a to ako kvalitatívnych, tak aj kvantitatívnych (finančné a ekonomické).

Kvantitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie výskytu rizika možnej škody zvýšením kybernetickej bezpečnosti

Kvalitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie miery rizika vzniku kybernetického incidentu.
- Zvýšenie miery súladu s platnou legislatívou.
- Zvýšenie úrovne kybernetickej a informačnej bezpečnosti.
- Zvýšenie detekcie kybernetických bezpečnostných incidentov.
- Zvýšená spokojnosť a dôvera používateľov.

Kalkulácia prínosov z pohľadu hodnoty v €

Z pohľadu monetizácie boli prínosy ocenená na cca 950 tis. € ročne, ako je vidieť v nasledujúcej tabuľke:

#	Názov prínosu	Popis	Ročná hodnota (€)	Metodika výpočtu a zdroje
1	Zníženie počtu bezpečnostných incidentov	Centralizácia dohľadu (SOC + SIEM + Threat Intelligence) umožní znížiť počet úspešných incidentov z 12 → 4 ročne.	90 000 €	Východiská: podľa CSIRT.SK 2023 priemer 8–15 incidentov/rok pre subjekty veľkosti NDS; priemerná škoda podľa ENISA ≈ 10 000 €/incident. Výpočet: (AS-IS 12 − TO-BE 4) × 10 000 € = 80 000 €, zaokrúhlené 90 000 € (pre zahrnutie sekundárnych efektov – menšie interné náklady na obnovu). Zdroje: ENISA Threat Landscape 2023; CSIRT.SK Správa o

				KB SR 2023; NIST SP 800-55 v2.
2	Skrátenie času detekcie a reakcie (MTTD/ MTTR)	Automatizácia procesov (SOAR, SIEM korelácie) skráti čas detekcie z 48 h → 6 h a reakcie z 24 h → 4 h. Rýchlejšia reakcia = menšie škody z výpadkov.	300 000 €	Východiská: 2 závažné incidenty ročne, dopad ≈ 5 000 €/ hod. (dokumentované náklady na výpadky podľa Gartner IT Infrastructure Downtime Cost Model 2021). Výpočet: AS-IS = 2 × (48 + 24) h × 5 000 €/ h = 720 000 €; TO-BE = 2 × (6 + 4) h × 5 000 € = 100 000 €; úspora ≈ 620 000 € → konzervatívne znížené na 300 000 € (pre realistický mix incidentov). Zdroje: Gartner 2021; ENISA CBA for Cybersecurity Projects (2021); NIST SP 800-55 v2 („Response Time Metric“).
3	Úspora interných kapacít (automatizácia + Service Desk)	Zjednotenie správy incidentov a automatizácia SOAR zníži manuálnu záťaž o 1,5 FTE.	90 000 €	Východiská: priemerná ročná mzda IT špecialistu v OVM = 60 000 € (Slovenský štatistický úrad 2024; priemer brutto + odvody). Výpočet: 1,5 FTE × 60 000 €/FTE = 90 000 €. Zdroje: ŠÚ SR – Priemerné mzdy v odvetví J62; NIST SP 800-55 v2 („Process Automation Efficiency“).
4	Zníženie neplánovaných výpadkov (NOC/APM)	Monitorovanie prevádzky a analyza anomálií (NOC) skráti neplánované výpadky o 20 %.	40 000 €	Východiská: AS-IS ≈ 40 h výpadkov ročne; dopad = 5 000 €/ h. Výpočet: AS-IS 200 000 € – TO-BE (32 h × 5 000 € = 160 000 €) = 40 000 €. Zdroje: Gartner IT Downtime Model (2021); ENISA Operational Resilience Report 2022.
5	Vyhnutie sa sankciám (NIS2/ZoKB)	Implementácia SOC, SIEM a správy rizík zabezpečí plnú zhodu so zákonom 69/2018 Z. z. a NIS2.	140 000 €	Východiská: Max. pokuty podľa §46 ZoKB = 200 000 €/ rok; pravdepodobnosť porušenia bez projektu ≈ 70 % (na základe NBU audits). Výpočet: 200 000 € × (0,7 – 0,05) = 130 000 €, zaokrúhlené 140 000 €. Zdroje: Zákon 69/2018 Z. z.; NIS2 Directive 2022/2555; NBÚ Výročná správa 2023.

6	Reputačný efekt (nižšie PR náklady)	Predídenie únikom dát a incidentom zníži riziko straty reputácie a PR nákladov.	50 000 €	Východiská: ENISA Cost of Breach 2023 – priemerné náklady na reputáciu ≈ 200 000 €; pravdepodobnosť znížená z 20 % → 5 %. Výpočet: 200 000 € × (0,2 − 0,05) = 30 000 € + odvrátené PR náklady ≈ 20 000 € = 50 000 €.
7	Efektívny asset a identity management (Exposure Mgmt)	Automatizované skenovanie aktív a inventarizácia zníži počet nevyužitých licencií.	70 000 €	Východiská: ročne spravované aktíva ≈ 1 000 000 €; nevyužitie AS-IS = 10 %, TO-BE = 3 %. Výpočet: (10 − 3) % × 1 000 000 € = 70 000 €. Zdroje: ISO 27005 Annex C (Asset Valuation); interné audity NDS.
8	Lepšie plánovanie a rozhodovanie (reporting)	Centralizovaný reporting zníži duplicitné nákupy a zlepší alokáciu zdrojov.	40 000 €	Východiská: ročne alokovaný bezpečnostný rozpočet ≈ 1 000 000 €; duplicitné projekty AS-IS = 8 %, TO-BE = 4 %. Výpočet: (8 − 4) % × 1 000 000 € = 40 000 €. Zdroje: NIST Cybersecurity Framework v1.1 (Identify/Govern & Risk Mgmt).
9	Zníženie ľudských chýb (štandardizácia + automatizácia)	Zavedenie štandardných procesov (ITIL/ISO 27001) zníži chybovosť pri zmene konfigurácií a správe systémov o 60 %.	130 000 €	Východiská: ≈ 200 chýb/rok z ľudskej chyby; 2 h náprava/chybu × 325 €/h (interné + externé náklady z finančných údajov NDS). Výpočet: 200 × 2 × 325 € × 60 % = 78 000 €; doplnkový efekt (oneskorenia, servisné zásahy) ≈ 50 000 €; spolu 130 000 €. Zdroje: ENISA Human Factor in Cyber Security 2022; NIST SP 800-55 v2.

3.7 Vyhodnotenie BC/CBA analýzy

V nasledujúcej tabuľke je vyhodnotená BC/CBA v horizonte 10 rokov:

	Cashflow projektu						Čistá súčasná hodnota z projektu				
	Finančný cashflow (s DPH)			Ekonomický cashflow (bez DPH)			koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návratnosť ENPV	
Obdobie	AS IS	TO BE	rozdiel	AS IS	TO BE	rozdiel					
t1	0,00	-1 404 900,00	-1 404 900,00	0,00	-220 750,00	-220 750,00	0	-1 404 900,00	-220 750,00	-220 750,00	<
t2	0,00	-1 115 676,00	-1 115 676,00	0,00	20 270,00	20 270,00	1	-1 072 765,38	19 304,76	-201 445,24	<
t3	0,00	-1 115 676,00	-1 115 676,00	0,00	20 270,00	20 270,00	2	-1 031 505,18	18 385,49	-183 059,75	<
t4	0,00	-1 115 676,00	-1 115 676,00	0,00	20 270,00	20 270,00	3	-991 831,90	17 509,99	-165 549,76	<
t5	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	4	-715 263,39	207 898,97	42 349,21	Rok návratu investície
t6	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	5	-687 753,26	197 999,02	240 348,23	>
t7	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	6	-661 301,21	188 570,50	428 918,73	>
t8	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	7	-635 866,55	179 590,95	608 509,68	>
t9	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	8	-611 410,14	171 039,00	779 548,67	>
t10	0,00	-836 757,00	-836 757,00	0,00	252 702,50	252 702,50	9	-587 894,37	162 894,28	942 442,96	>
SPOLU	0,00	-9 772 470,00	-9 772 470,00	0,00	1 356 275,00	1 356 275,00	SPOLU	-8 400 491,39	942 442,96		

Výsledok CBA		Výsledná hodnota	minimálna hodnota
BCR	pomer prínosov a nákladov	0,95	1,00
FIRR	finančná vnútorná výnosová miera (%)	N/A	-
EIRR	ekonomická vnútorná výnosová miera (%)	41,4%	5,0%
FNPV	finančná čistá súčasná hodnota (eur s DPH)	-8 400 491	-
ENPV	ekonomická čistá súčasná hodnota (eur bez DPH)	942 443	0

Zvislá (Kategória) Os

3.8 HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza	08/2025	09/2025	
2.	Iniciačná fáza	10/2025	12/2025	
3.	Realizačná fáza	01/2026	12/2029	
3a	Analýza a Dizajn	01/2026	05/2026	Je známa počas príprav obstarávania na základe auditnej správy
3b	Nákup technických prostriedkov, programových prostriedkov a služieb	06/2026	10/2026	
3c	Implementácia a testovanie	11/2026	12/2026	
3d	Nasadenie a PIP	01/2027	12/2029	
4.	Dokončovacia fáza	01/2027	12/2029	
5.	Podpora prevádzky (SLA)	01/2030	02/2033	

Projekt bude realizovaný jedným inkrementom metódou waterfall.

3.9 Návrh organizačného zabezpečenia projektu (projektový tím)

Bude zostavený riadiaci výbor (RV), v minimálnom zložení:

- Predseda RV
- zástupca vlastníkov procesov objednávateľa
- zástupca kľúčových používateľov objednávateľa
- zástupca dodávateľa (doplňa sa až po VO / voliteľný člen)

Bude zároveň stanovený PM objednávateľa a zostavený nasledujúci projektový tím:

- kľúčový používateľ,
- IT analytik,
- IT architekt,
- manažér kvality,
- vlastník procesov

- manažér kybernetickej a informačnej bezpečnosti
- špecialista kybernetickej bezpečnosti,
- špecialista pre bezpečnosť prevádzky systémov

Projektový tím bude pokrytý existujúcimi kapacitami a preto v rámci CBA nie sú kalkulované náklady na potrebu interných zdrojov.

Zároveň sa predpokladá zloženie tímu dodávateľa v nasledujúcom rozsahu, pričom presnán špecifikácia pozícií bude predmetom VO:

- IT analytik
- IT programátor/vývojár
- Projektový manažér IT projektu
- Špecialista pre databázy
- IT architekt
- Špecialista pre infraštruktúrny/HW špecialista
- Špecialista pre bezpečnosť IT

Zároveň sú požiadavky na dodávateľa uvedené v časti 8 Prevádzka a údržba.

Konkrétne mená pre interný, ako aj externý tím budú doplnené v čase ukončenia VO.

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte
2.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte
3.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte

3.10 Pracovné náplne

Pracovné náplne budú definované v zmysle šablón uvedených na nasledujúcom odkaze: https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html

4. Legislatíva

Projekt musí byť realizované v súlade s minimálne nasledovnými predpismi:

1. **Predpisy v oblasti kybernetickej bezpečnosti**

1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých predpisov
2. Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov
3. Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
4. Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
5. Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a všetkých ďalších predpisov

1. **GDPR**

1. Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
2. Nariadenie Európskeho parlamentu a Rady 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES

1. **ITVS (informačné technológie vo verejnej správe)**

1. Zákon č. 95/2019 Z. z., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov
2. Vyhláška Úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
3. Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
4. Vyhláška Úradu podpredsedu vlády SR pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Pre potreby realizácie projektu nie je potrebná žiadna legislatívna zmena

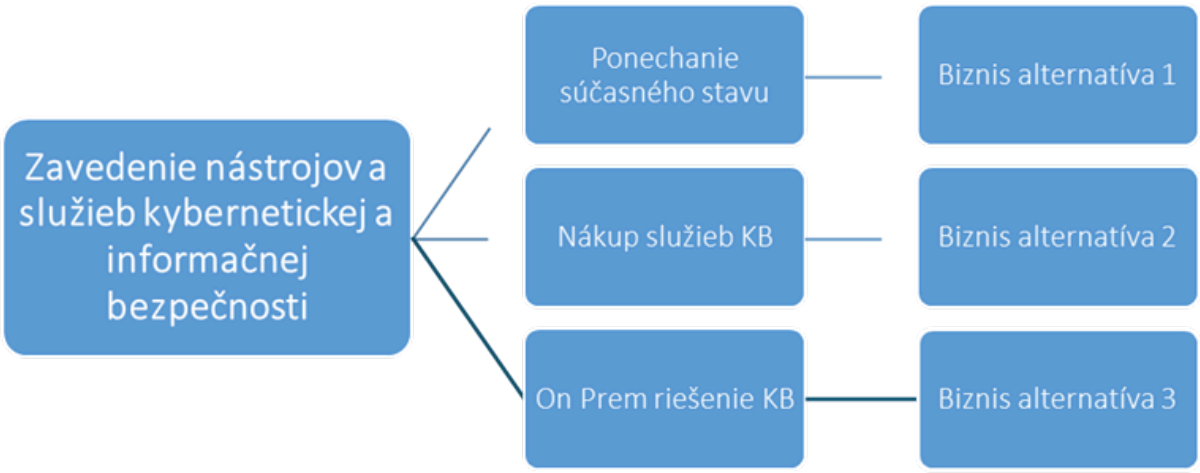
5. Architektúra riešenia projektu

5.1 Alternatívy a MCA

V tejto časti sú popísané a vyhodnotené jednotlivé varianty, ktoré boli zavažované

5.1.1 Stanovenie alternatív pomocou biznisovej vrstvy architektúry

V rámci biznisovej vrstvy architektúry sme porovnávali 3 variantné alternatívy riešenia súčasného stavu. Na základe identifikovaného rozsahu problému v projektovom zámere boli stanovené tri rôzne riešenia. Ako najefektívnejšia bola vybraná Alternatíva č. 3 taká, kt. pokrýva procesy a požiadavky všetkých stakeholderov.



V nasledujúcej tabuľke je stručný popis jednotlivých alternatív:

Alternatíva	Popis
Ponechanie AS IS stavu	Jedná sa o situáciu, kedy sa nič nebude meniť. Ostane zachovaná funkčnosť, ktorá je implementovaná v súčasnosti a to v nasledovnom rozsahu: • Antivirus pre pracovné stanice a serveri • Firewall pre NW segmenty • DLP • MFA • Endpoint Management • Iné

Nákup služieb KB	Organizácia nekupuje softvér ani infraštruktúru do vlastníctva. Bezpečnostné technológie (uvedené v časti 3.1.5 Rozsah projektu) sú poskytované formou služby na základe pravidelného poplatku (OPEX). Dodávateľ zodpovedá za prevádzku, aktualizácie, patchovanie, zabezpečenie, SLA, škálovanie a expertov. Vlastnosti: • Prevádzka aj údržba sú poskytované ako služba. • Aktualizácie a hrozbové dáta (IoC, TI feedy) sú v cene. • Rýchla integrácia multivendor nástrojov. • Predvídateľné náklady, škálovanie podľa potreby. • Nižšie nároky na interný personál. • Garantované reakčné časy a špecialisti (SOC/MSSP).
On Premise riešenie KB	Organizácia kupuje softvérové licencie do vlastníctva, prevádzkuje ich na svojej infraštruktúre a zabezpečuje vlastných špecialistov pre správu, monitoring, konfigurácie, threat hunting a reakciu na incidenty. Dodávateľ dodá len licencie a prípadne základnú implementáciu. Vlastnosti: • Vyžaduje vlastné servery, úložiská, backup, sieťovú techniku. • Organizácia musí realizovať aktualizácie, patching a tuning. • SOC tím a bezpečnostný dohľad musia byť interné alebo osobitne obstarané. • Náklady sú prevažne CAPEX + vysoké interné OPEX.

5.1.2 Definovanie požadovaného stavu

- Exposure and Risk management
  - Nástroj pre detekciu Internal Attack Surface, Vulnerability Management
  - Nástroj pre detekciu External Attack Surface
  - Nástroj pre Exposure Management
  - Nástroj pre Risk Management a SIEM
  - Nástroj pre Digital Risk Protection
  - Nástroj pre DAST development
  - Nástroj pre Cloud Posture
  - Nástroj pre Threat Intelligence (Tactical and Operational Intelligence)
  - Nástroj pre správu IoC
  - Nástroj pre Threat Thisd Party overovanie
  - Nástroj pre Security Orchestration and Reposnse Automation
- Service Desk (ITIL)
  - Nástroj pre Incident Management
  - Nástroj pre Change Management
  - Nástroj pre Problem Management
  - Nástroj pre Request Management
  - Nástroj pre Risk Management (netechnický)
  - Nástroj pre Servis Catalog
- Nástroj pre NOC (Network Operation Center)
  - Mirrovanie komunikácie na sieti a jej nezávislé vyhodnocovanie podľa preddefinovaných IoC ako aj vlastných reťazcov
  - Sledovanie výkonnosti aplikácií
  - behaviorálna analýza komunikačných zmien a detekcia anomálií

- SOC services
    - Vyhodnocovanie zozbieraných logov z bezpečnostných technológií, aplikácií, operačných systémov, siete.
    - Preverovanie hlásení a filtrovanie „False Positive“
    - Kontrola zmien na systémoch oproti Service Desk
    - Incident response
    - Forenzná analýza bezpečnostných incidentov
    - Právne a masmediálne poradenstvo tákajúce sa bezpečnostných incidentov
    - hlásenie incidentov na relevantné orgány (NBU, CSIRT)
    - evidencia a spolupráca pri vyšetrovaní incidentov s nadnárodnými organizáciami
    - poradenstvo v prevencii a prípadné vypracovanie bezpečnostných projektov vyplývajúcich z bezpečnostných incidentov

5.1.3 Multikriteriálna analýza

V nasledujúcej tabuľke sú stanovené kritéria pre vyhodnotenie alternatív:

	KRITÉRIUM	ZDÔVODNENIE KRIÉRIA	IT prevádzka	MKB	Štatutár	CFO & HR	Users	CSIRT & NBU
BIZNIS VRSTVA	K1 – Súlad s legislatívou a bezpečnostnými štandardmi (ZoKB, NIS2, NBÚ 362/2018, GDPR, CIS Controls)	Projekt zabezpečuje kybernetickú ochranu kritickej infraštruktúry, ktorá musí spĺňať zákonné požiadavky. Riešenie musí umožniť auditovateľnosť, reporting, logovanie a schopnosť preukázať súlad.	X	X	X	X		X
	K2 – Dostupnosť expertných kapacít a 24/7 dohľadu	Kybernetická bezpečnosť vyžaduje nepretržitý monitoring a kvalifikovaných analytikov L1–L3. Interné kapacity NDS sú nedostatočné, čo je uvedené v OPZ. Bez expertného tímu nie je možné zabezpečiť reakciu na incidenty.	X	X	X	X		X
	K3 – Čas implementácie a dosiahnutie	Projekt je časovo citlivý vzhľadom na hrozby,	X	X	X	X	X	

funkčného stavu	ktoré môžu vzniknúť už počas implementácie. Rýchle spustenie SOC a monitoringu výrazne znižuje vystavenie rizikám.							
K4 – Flexibilita a škálovateľnosť riešenia	Počet zariadení (10 000+) a užívateľov (1 200) môže rásť. Riešenie musí umožniť postupné dokupovanie licencií, pokrytie pripravovaných cloud služieb a rozšírenie do nových segmentov siete.	X		X		X		X			
K5 – Bezpečnostná efektívnosť (kvalita detekcie, reakcie, threat intelligence, automatizácia)	Rozhodujúce kritérium pre dosiahnutie cieľov projektu – minimalizovať čas detekcie, eliminovať falošné poplachy, využívať TI feedy a SOAR automatizáciu. Zásadne ovplyvňuje schopnosť predchádzať incidentom.	X		X		X			X		X
K6 – Prevádzkové riziká pre organizáciu (záťaž na IT, riziko neaktuálnosti, závislosť od interných kapacít)	Toto kritérium hodnotí mieru prevádzkovej náročnosti, ktorú jednotlivé alternatívy kladú na organizáciu. Posudzuje sa potreba interných	X		X		X		X			X

kapacít, komplexita prevádzkovej podpory, požiadavky na zabezpečenie aktualizácií, údržbu technológií, správu konfigurácií, ako aj administratívne a procesné dopady spojené s prevádzkovaním riešenia. Kritérium tak umožňuje porovnať dlhodobú udržateľnosť jednotlivých variantov z pohľadu organizácie.

Pre potreby hodnotenia bola zvolená nasledovná metodika:

- Stanovenie váhy kritéria:
  - K1 – Súlad s legislatívou a bezpečnostnými štandardmi (váha 25 %)
  - K2 – Dostupnosť expertných kapacít a 24/7 dohľad (KO + váha 20 %)
  - K3 – Čas implementácie a dosiahnutie plnej funkčnosti (váha 15 %)
  - K4 – Flexibilita a škálovateľnosť riešenia (váha 10 %)
  - K5 – Bezpečnostná efektívnosť (kvalita detekcie a reakcie) (váha 20 %)
  - K6 – Prevádzkové riziká pre organizáciu (váha 10 %)
- Bodovanie splnenia kritéria:
  - 1 – veľmi zlé
  - 2 – slabé
  - 3 – priemerné
  - 4 – dobré
  - 5 – výborné

V nasledujúcej tabuľke je vyhodnotenie splnenia kritérií podľa jednotlivých variant

	Alternatíva 1		**Alternatíva 3**		**Alternatíva 2**	
	Hodnota	**Odôvodnenie**	**Hodnota**	**Odôvodnenie**	**Hodnota**	**Odôvodnenie**
K1	**1**	Neplní ZoKB, NIS2, NBÚ 362/2018	3	Možno splniť, ale s náročnými investíciami a údržbou	5	Najvyššia miera compliance – automatizované aktualizácie, TI, reporting
K2	**1**	Žiadny odborný dohľad, chýbajú experti	2	Potreba viacero FTE, nedostatok odborníkov na trhu	5	24/7 SOC, L1–L3 analytici, garantované SLA
K3	**5**	Stav existuje – nulová implementácia	2	Implementácia 18–36	4	Implementácia 3–6 mesiacov

				mesiacov (SOC)			
K4	**1**	Nedá sa škálovať, chýbajú integračné body	3	Škálovateľnosť limitovaná HW a licencovaním	5	Okamžité škálovanie, licencie podľa potreby	
K5	**1**	Minimálna detekcia, žiadna korelácia	3	Dobrá efektivita, ale závislá od interného tímu	5	Najvyššia úroveň detekcie a reakcie, TI feedy, SOAR automatizácia	
K6	**1**	Vysoké riziko incidentov, chýba monitoring	2	Veľká prevádzková záťaž, riziko neaktuálnych systémov	4	Nízka prevádzková záťaž, minimálne riziko zastarania	

Porovnanie:

- AS-IS: 1.60 / 5 – nevyhovuje legislatíve, vysoké bezpečnostné riziká
- Subscription model: 4.75 / 5 – najlepšie spĺňa biznis aj bezpečnostné požiadavky
- On-prem: 2.55 / 5 – splniteľné, ale náročné na personál, čas a údržbu

5.1 4 Stanovenie alternatív pomocou aplikačnej vrstvy architektúry

Ponechanie existujúceho stavu: Existujúci stave nespĺňa požiadavky na multi-vendor stratégiu. Je neprofesionálne pre kritickú infraštruktúru sa spoliehať výhradne na jedného dodávateľa bezpečnostnej technológie ako aj na jej správnu konfiguráciu a dohľad. Základ aktívnej bezpečnosti je postavený na Fortinet zariadeniach, pričom Fortinet ma najvyšší počet objavených bezpečnostných zraniteľností. Vzhľadom na finančnú a časovú obťažnosť nahradenia tejto technológie je bezpečnejšie zabezpečiť nezávislú kontrolu a vyhodnocovanie internej siete a to hlavne za predpokladu, že výrobca sa aj napriek vysokému počtu zraniteľností radí medzi technologickú špičku. Obdobne je to aj s Antivírovým riešením, ktoré je všeobecne neodporúčané (Kaspersky), pričom dosahuje svoje kvality. Ponechanie existujúcich riešení bez dodatočných investícií na rozvoj nie je v súlade s legislatívnou úpravou Zákona o Kybernetickej Bezpečnosti, neumožňuje evidenciu a komplexnú identifikáciu rizík. V existujúcom stave nie je dostatok expertných ľudských zdrojov na prevádzku dohľadu nad bezpečnosťou so schopnosťou reagovať na prípadné incidenty. Doplnenie tohto stavu z externých zdrojov nie je dostatočné bez potrebných nezávislých nástrojov, ktoré expertní pracovníci ovládajú a dôverujú im.

Využitie open source a vlastných síl: Implementácia a údržba open source riešení je často spojená s negarantovanou kvalitou a vyššími nárokmi na ľudské zdroje. Interne nedisponujeme kapacitami pre pokrytie bezpečnostného monitoringu, preto máme záujem obstarať prioritne bezpečnostný dohľad ako službu, pričom open source je akceptovaný ako súčasť dodávky v rámci služby. V rámci prieskumu Open Source riešení na obstarávané technológie a ich schopnosti detekcie silno neodporúčame požitie verejných zdrojov pre identifikáciu škodlivého kódu a komunikácie vzhľadom na ich nedostatočnú schopnosť eliminovať falošné stopy (false positive). Napr. generic SNORT, YARA pravidla z voľne dostupných zdrojov ako aj IoC na báze STIX / TAXII, ktoré vykazujú vysokú nespoľahlivosť. Tieto technológie používame aj ako doplnok existujúcich riešení a práve na popísané nedostatky požadujeme rozšírený threat intelligence pre identifikáciu dôveryhodnosti a správnosti verejných zdrojov pre open source riešenia.

Použitie komerčných produktov: Primárne obstarávame službu a definujeme, čo musí obsahovať. Potrebné nástroje pre dodávku požadovanej služby chceme obstarať hlavne pre prípad skončenia poskytovania služby, ktoré potenciálne by sme vedeli nahradiť z vlastných zdrojov po zamestnaní požadovaných expertov. Neuvažujeme primárne so zvyšovaním ľudských zdrojov pre expertné funkcie dohľadu nad bezpečnosťou vzhľadom na fakt, že interne by sme nedokázali plne využiť ich potenciál a prenájom tohto kvalifikovaného personálu je lacnejší.

5.1.5 Stanovenie alternatív pomocou technologickej vrstvy architektúry

Vzhľadom na zvolenú biznis alternatívu bude technologická vrstva pre riešenie zabezpečená na strane dodávateľa

5.2 POŽADOVANÉ VÝSTUPY – projektový popis produktu

TO BE:

•

Požadovaný stav:

- Exposure and Risk management
  - Nástroj pre detekciu Internal Attack Surface, Vulnerability Management
  - Nástroj pre detekciu External Attack Surface
  - Nástroj pre Exposure Management
  - Nástroj pre Risk Management a SIEM
  - Nástroj pre Digital Risk Protection
  - Nástroj pre DAST development
  - Nástroj pre Cloud Posture
  - Nástroj pre Threat Intelligence (Tactical and Operational Intelligence)
  - Nástroj pre správu IoC
  - Nástroj pre Threat Thisd Party overovanie
  - Nástroj pre Security Orchestration and Reposnse Automation
- Service Desk (ITIL)
  - Nástroj pre Incident Management
  - Nástroj pre Change Management
  - Nástroj pre Problem Management
  - Nástroj pre Request Management
  - Nástroj pre Risk Management (netechnický)
  - Nástroj pre Servis Catalog
- Nástroj pre NOC (Network Operation Center)
  - Mirrovanie komunikácie na sieti a jej nezávislé vyhodnocovanie podľa preddefinovaných IoC ako aj vlastných reťazcov
  - Sledovanie výkonnosti aplikácií
  - behaviorálna analýza komunikačných zmien a detekcia anomálií
- SOC services
  - Vyhodnocovanie zozbieraných logov z bezpečnostných technológií, aplikácií, operačných systémov, siete.
  - Preverovanie hlásení a filtrovanie „False Positive“
  - Kontrola zmien na systémoch oproti Service Desk
  - Incident response
  - Forenzná analýza bezpečnostných incidentov
  - Právne a masmediálne poradenstvo tákajúce sa bezpečnostných incidentov
  - hlásenie incidentov na relevantné orgány (NBU, CSIRT)
  - evidencia a spolupráca pri vyšetrovaní incidentov s nadnárodnými organizáciami
  - poradenstvo v prevencii a prípadné vypracovanie bezpečnostných projektov vyplývajúcich z bezpečnostných incidentov

Predmetom projektu je zabezpečenie doplnkových činností v oblasti kybernetickej a informačnej bezpečnosti v organizácii a zabezpečenie vybraných činností zameraných na prevenciu pred kybernetickými bezpečnostnými incidentmi v organizácii žiadateľa konkrétne:

-
  - Centralizácia pre zobrazenie, kategorizáciu a prioritizáciu rizík (Exposure and Risk Management)
  - Evidencia požiadaviek a incidentov v centrálnom nástroji (Service Desk)
  - Rozšírený monitoring sieťovej prevádzky a dohľadové centrum (Nástroj pre NOC)
  - Outsourcing bezpečnostných služieb pre urýchlenú identifikáciu hrozby a odstránenie rizika (SOC services)

Danými nástrojmi spolu s existujúcim riešením dokážeme zabezpečiť súlad zo zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“), ako aj doplniť konzistenciu odporúčaní podľa CIS framework v nasledujúcich oblastiach:

- (CIS Control 1) Inventarizácia zariadení pristupujúcich k aplikáciám a dátam
- (CIS Control 2) Kontrola zariadení pristupujúcich k dátam a aplikáciám na vyžadované bezpečnostné štandardy a izoláciu dát

- (CIS Control 5) Evidencia účtov, auditné logy a správa oprávnení a to v rátane Cloud prostredia
- (CIS Control 7) Kontinuálna správa zraniteľností na všetkých prvkoch infraštruktúry v rátane pracovných staníc
- (CIS Control 8) Archivácia a vyhodnocovanie auditných logov
- (CIS Control 10) Ochrana proti škodlivým kódom na všetkých vrstvách
- (CIS Control 13) Dohľadová úroveň bezpečnosti sieťových zariadení a toku dát
- (CIS Control 15) Zabezpečenie aplikácií a dát v externom prostredí
- (CIS Control 16) Bezpečnosť aplikácií
- (CIS Control 17) Schopnosť detegovať a reagovať na bezpečnostné incidenty
- (CIS Control 18) Penetračné testovanie po technickej stránke.

Odvolávka na CIS framework je z dôvodu, že prevažná väčšina bezpečnostných nástrojov má integrované minimálne CIS normy vo svojich politikách a pravidlách pre vyhodnocovanie zhody s požadovanými nastaveniami, ktoré sú v súlade s platnou legislatívnou úpravou:

- Zákon č. 69/2018 Z.z . o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 287/2021 Z. z. Zákon, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony
- Zákon č. 95/2019 Z.z . informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Vyhláška NBÚ č. 362/2018 Z.z . ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- vyhlášky NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
- vyhlášky NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
- zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o doplnení niektorých zákonov,
- zákona č. 45/2011 Z. z. o kritickej infraštruktúre,
- zákona č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov (GDPR),
- zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- Zákon č. 56/2018 Z.z . o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov
- ISO/IEC 17024:2012 Posudzovanie zhody Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb
- ISO/IEC 17000:2020 Posudzovanie zhody Slovník a všeobecné zásady
- ISO/IEC 27000 „Informačné technológie Bezpečnostné metódy Systémy riadenia informačnej bezpečnosti“,
- Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 (NIS2) o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
- nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
- zákona č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov,
- smernice Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) a jej implementácie v zákone č. 351/2011 Z. z. o elektronických komunikáciách
- nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické

5.3 Náhľad architektúry

Architektúra riešenia projektu je spracovaná v súlade s hlavnými cieľmi, ktoré sú podrobnejšie definované funkčnými resp. nefunkčnými požiadavkami uvedené v prílohe Opis Predmetu Zákazky. Architektúra riešenia projektu je ďalej rozpracovaná na úrovni biznis vrstvy, aplikačnej vrstvy, technologickej vrstvy a bezpečnostnej vrstvy z prihliadnutím na minimalizovanie počtu potrebných nástrojov a výrobcov, pričom dôraz je na univerzálnosť

implementácie nástrojov do heterogénneho prostredia z pohľadu prepojiteľnosti cloud a onprem prostredí, platformovú univerzálnosť a aplikačnú nezávislosť. Navrhované riešenie rozširuje existujúcu bezpečnosť postavenú na produktoch prioritne ForcePoint, Thales, Fortinet, Kaspersky, Veeam, Kronos, a iné.

5.3.1 Biznis vrstva

AS IS: Existujúce prostredie spočíva v mikrosegmentovanej sieti, pričom majoritné sú dve lokality. Pre tieto 2 lokality je nutné riešiť detailnejšie sieťový monitoring, v týchto dvoch lokalitách sa nachádza prevažná väčšina administratívnych PC, užívateľov a serverov a nimi poskytovaných služieb. Dominantná platforma v rámci administratívnej siete je Microsoft Windows. Okrem on-prem infraštruktúry je v blizkej dobe plánované rozšírenie do verejného Cloud prostredia vo forme hostovaného Workload, ale aj vo forme SaaS služieb (používame Office 365, plánované sú migrácie niektorých služieb z vnútorného prostredia). Zbytok siete pozostáva z microsegmentov prevažne pre IoT a OT zariadenia. Všetky siete sú navzájom prepojené a zabezpečené firewallom. Celkový počet užívateľov je 1200, celkový počet TCP/IP zariadení je 10000. Vyžíva sa približne 100 aplikácií a služieb.

TO BE: Cieľom je doplniť v rámci multivendor strategy bezpečnostné technológie a spolu s existujúcimi ich napojiť na centrálny bod pro organizáciu poskytujúcu bezpečnostný dohľad na výkonnosťou aplikácií, bezpečnosťou komunikácie ako aj bezpečnosťou samotných pracovných staníc, serverov a cloud prostredia.

5.3.2 Prehľad koncových služieb – budúci stav:

Projektom nie sú budované žiadne nové koncové služby. Cieľom projektu je sledovať funkčnosť a výkonnosť služieb, identifikovať čo najskôr možné riziko a to na proaktívnej ako aj reaktívnej úrovni, zvýšenie kybernetickej a informačnej bezpečnosti a schopnosti identifikovať incidenty aj pri zlyhaní primárnej existujúcej bezpečnostnej technológie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

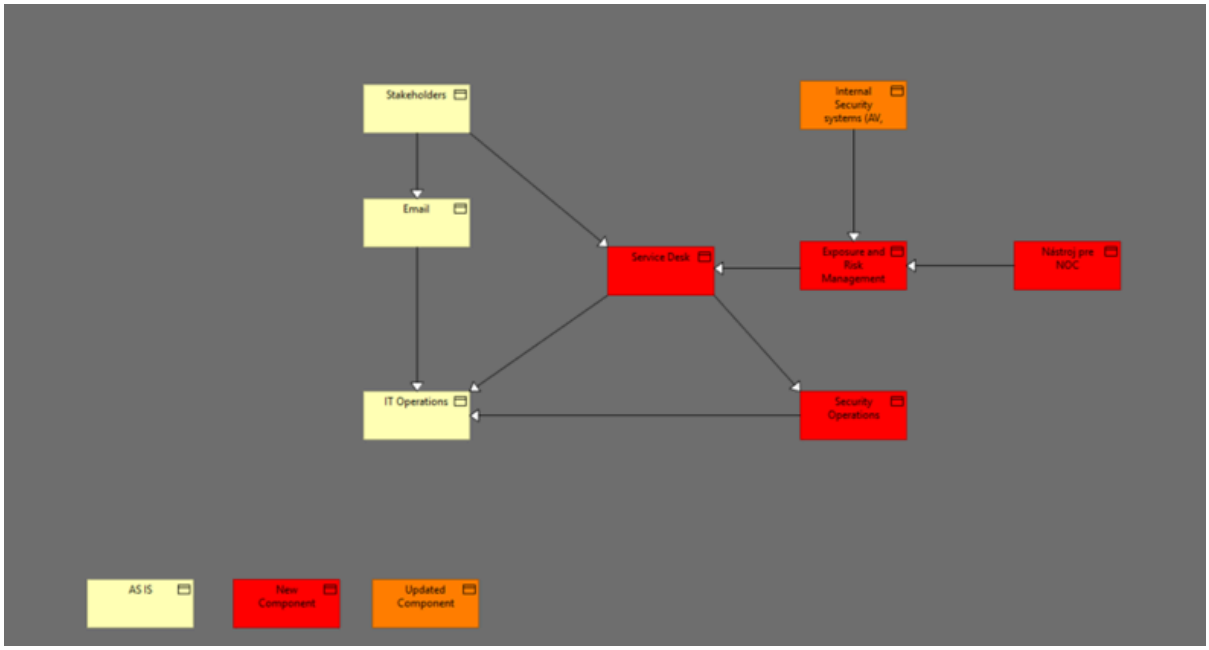
5.3.3 Jazyková podpora a lokalizácia

Všetky požadované technológie musia byť dostupné v Slovenskom alebo Anglickom jazyku vrátane dokumentácie výrobcu. Projektová dokumentácia bude vypracovaná v Slovenskom jazyku.

5.4 Aplikačná vrstva

Aplikačná vrstva pozostáva z približne 100 aplikácií, od bežných administratívnych (Exchange, Sharepoint, ERP, CRM, KMS, ...) cez operatívne web aplikácie aplikácie na platformách IIS, Apache (dochádzky, dovolenky, schvaľovacie postupy, žiadosti nákupu a prevádzkové postupy a iné), pre plánovanie a optimalizovanie prevádzky až po samotné prevádzkové aplikácie (SCADA). Samotná SCADA sieť nie je primárnym predmetom monitoringu.

Zmeny nastávajú iba po procesnej stránke zavedením systému na evidenciu požiadaviek a asetov.



5.4.1 Rozsah informačných systémov – AS IS

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

Kód ISVS (z MetaIS)	Názov ISVS	Modul ISVS (zaškrtnite ak ISVS je modulom)	Stav IS VS (AS IS)	Typ IS VS	Kód nadradeného ISVS (v prípade zaškrtnutého checkboxu pre modul ISVS)
		#	Vyberte jednu z možností	Vyberte jednu z možností	
		#	Vyberte jednu z možností	Vyberte jednu z možností	

5.4.2 Rozsah informačných systémov – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

V rámci projektu budú implementované nové nástroje pre zvýšenie úrovne kybernetickej a informačnej bezpečnosti a evidencie rizík.

5.4.3 Využívanie nadrezortných a spoločných ISVS – AS IS

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.4 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.5 Prehľad plánovaného využívania iných ISVS (integrácie) – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.7 Aplikačné služby na integráciu – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

Projektom nie je plánované poskytovanie údajov do IS CSRŮ.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.4.9 Konzumovanie údajov z IS CSRU – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5 Dátová vrstva

Samotný projekt nemení existujúcu dátovú vrstvu z pohľadu obsahu, doplňuje nástroje pre včasnú identifikáciu rizík. Existujúce dáta ani technológie sa nemenia, a rovnako sa neplánuje modifikovať dátovú vrstvu. Metadáta z jednotlivých nástrojov, ako sú napríklad logy z existujúcich bezpečnostných technológii plánujeme preposielať do centrálneho systému (SIEM), ktorý je predmetom obstarávania a mal by zabezpečovať včasne upozornenie na koreláciu podozrivých aktivít. Sada nástrojov, ktoré sú predmetom projektu by nemala byť prioritne závislá na preposielaných logoch, ale hlavne na aktívnych komponentoch, ktoré generujú vlastné dáta (napríklad sonda v sieti, nezávislý EDR/XDR agent, atď). V OPZ budú definované bezpečnostne požiadavky na obstarávané nástroje či už z pohľadu dodržiavania štandardov pre prístup k zozbieraným údajom (RBAC), ich prenosu (TLS) alebo samotnej správe takto zozbieraných údajov (GDPR, audit, a iné normy alebo certifikácie). Umiestnené budú tak ako doteraz v infraštruktúre NDS a.s. a pristupovať k nim budú tak ako doteraz oprávnení zamestnanci NDS a.s. a na základe poskytovania služby SIEM oprávnení zamestnanci dodávateľa.

5.5.1 Údaje v správe organizácie

Zavedenie systematického manažmentu údajov nie je predmetom navrhovaného projektu.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.3 Referenčné údaje

Projektom nie sú plánované žiadne nové referenčné údaje ani údaje, ktoré je možné vyhlásiť za referenčné.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.4 Kvalita a čistenie údajov

Cieľom projektu nie je systematický manažment údajov z hľadiska citlivosti kvality údajov a čistenia údajov.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.5 Analytické údaje

Nie je relevantné pre projekt, nebudú poskytované žiadne nové Analytické údaje.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.6 Moje údaje

Nie je relevantné pre projekt, nebudú poskytované žiadne nové Moje údaje.

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.5.7 Prehľad jednotlivých kategórií údajov

Projekt nie je zameraný na systematický manažment údajov, nemení štruktúru ani obsah údajov. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

5.6 Technologická vrstva

5.6.1 Prehľad technologického stavu - AS IS

Pripojenie celej sieťovej infraštruktúry zabezpečené pomocou NG FW služieb a dodatočne chránené prostredníctvom S2S VPN. Operačné systémy sú chránené Antivírovým programom.

5.6.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Navrhované nástroje budú bežať na infraštruktúre objednávateľa, prípadne na dedikovanom dodanom hardware alebo ako súčasť aplikácií poskytovaných z cloudu výrobcu. Navýšenie výkonu infraštruktúry nie je súčasťou projektu. Prípadné potrebné navýšenie výpočtového výkonu bude riešené osobitne v čase podľa potrieb.

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	1200	1200	Nemenia sa predpoklady
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	1200	1200	Nemenia sa predpoklady

Počet externých používateľov (internet)	1000	1000	Nemenia sa predpoklady
Počet externých používateľov používajúcich systém v špičkovom zaťažení	NA	NA	Nemenia sa predpoklady
Počet transakcií (podaní, požiadaviek) za obdobie	NA	NA	Nemenia sa predpoklady
Objem údajov na transakciu	NA	NA	Nemenia sa predpoklady
Objem existujúcich kmeňových dát	NA	NA	Nemenia sa predpoklady
Počet zariadení	10000	10000	NDS sídli aktuálne vo viac ako 25 lokalitách a infraštruktúru má vo viacerých dátových centrách. Všetky zariadenia pripojené v MPLS NDS a.s. - Endpointy (pracovné stanice, notebook, tablety, mobilné zariadenia, zobrazovacie jednotky), sieťové tlačiarne, všetky sieťové prvky a sieťová infraštruktúra, servre, NVRka a kamery

5.6.3 Návrh riešenia technologickej architektúry

Technologická architektúra sa oproti súčasnému stavu nemení a bude prevádzkovaná v rovnakom technologickom prostredí. Technologická vrstva budúceho stavu vychádza zo súčasného stavu a bude podporená novými nasadenými bezpečnostnými nástrojmi prevádzkovanými na viacerých technológiách.

5.6.4 Využívanie služieb z katalógu služieb vládneho cloudu

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie vrátane poskytovaných služieb z vládneho Cloudu. Práve vďaka decentralizácii prístupov a hostingových služieb nerozdeľujeme aplikácie podľa umiestnenia v hostingu, čo naopak umožňuje jednoduchšiu migráciu aplikačných celkov do prostredia vládneho cloudu.

5.7. Bezpečnostná architektúra

Samotná realizácia projektu definuje bezpečnostnú architektúru

6. Závislosti na ostatné ISVS / projekty

Predkladaný projekt nie je závislý na iných pripravovaných resp. prebiehajúcich projektoch.

7. Zdrojové kódy

Projekt nezahŕňa vývoj alebo dodanie vlastného informačného systému ani proprietárneho zdrojového kódu na mieru objednávateľa. Predmetom projektu je poskytovanie bezpečnostných nástrojov a služieb kybernetickej bezpečnosti na časovo obmedzené obdobie. Zároveň je projekt realizovaný na časovo obmedzené obdobie, pričom nedochádza k vytváraniu trvalej závislosti na jednom dodávateľovi

Všetky výstupy vzniknuté v rámci realizácie projektu, najmä:

- bezpečnostné logy a dáta,
- konfiguračné nastavenia bezpečnostných nástrojov,
- detekčné pravidlá, korelačné scenáre a politiky,
- automatizačné a reakčné playbooky (SOAR),
- prevádzková, bezpečnostná a projektová dokumentácia,

budú výhradným vlastníctvom Národnej diaľničnej spoločnosti a budú jej odovzdané v elektronickej podobe.

Dodávateľ je povinný zabezpečiť, aby všetky relevantné výstupy a dáta boli dostupné a exportovateľné v bežne používaných, otvorených alebo štandardizovaných formátoch, ktoré umožnia ich ďalšie využitie alebo migráciu k inému poskytovateľovi bezpečnostných služieb.

Po ukončení projektu bude mať objednávateľ k dispozícii kompletnú dokumentáciu a dátové výstupy potrebné na plynulé prevzatie riešenia alebo jeho pokračovanie s iným dodávateľom, čím sa minimalizuje riziko vendor lock-in.

8. Prevádzka a údržba

Prevádzka a údržba navrhnutého riešenia projektu je v plnom rozsahu predmetom obstarávania. Neuvažuje sa s využitím interných ľudských zdrojov. Monitoring služby majú za úlohu upozorniť na možné a prebiehajúce identifikované riziká. Možnosť odstránenia rizík ako aj prípadných následkov bude čerpaná výhradne na predošlý písomný súhlas. Počas trvania projektu a zavádzania SOAR automatizácie bude postupne upravovaná RACI matica, ktorá bude postupne pridávať právomoci pre SOC team.

8.1 Prevádzkové požiadavky

Prevádzkové požiadavky sú predmetom obstarania, ako správa bezpečnostných systémov, tak aj monitoring, reporting a interpretácia dát. Bližšia špecifikácia je rozpísaná vo Funkčných a nefunkčných požiadavkách obsiahnutých v opise predmetu zákazky.

V nasledujúcej tabuľke sú uvedené základné požiadavky, ktoré sú predmetom obstarávania:

Exposure and Risk mgmt:

Support	Podpora dodávateľa je dostupná priamo v nástroji (dokumentácia, pomoc, žiadosti o podporu). Podpora 7x24 pre platformu. Voliteľná podpora dodávateľa pre DÁTA (nie platformu samotnú) / spravované služby. Manuály k produktu sú verejne dostupné. Verejne dostupná diskusná platforma moderovaná dodávateľom. Informácie o vydaniach a aktualizáciách sú viditeľné priamo na platforme.

Nástroje pre NOC:

support	zákaznícka podpora po telefóne a emailom v českom alebo slovenskom jazyku od pondelka do nedele (24x7), prístup k webovému zákazníckemu centru, vzdialená podpora cez SSH. Výmena HW 24x7xNBD.

SOC services:

daily operations (L1 support)	Basic Monitoring	system checkup	kontrola funkčnosti zberu logov kontrola systémových parametrov komponentov riešenia kontrola funkčnosti generovania definovaných reportov
	Basic Analysis	Investigation Analysis	investigácia korelovaných alertov a vzniknutých incidentov

		Alerts trackdown	kontrola indikátorov stavu ohrozenia, eliminácia falošných správ
		Events Classification and Enrichment	klasifikácia udalostí podľa dopadu na prostredie a doplnenie rozšírených údajov
	Reporting	Notifications	upozornenie zákazníka a prípadná eskalácia na hĺbkovú inšpekciu
	SLA	response times	začatie vyšetrovania na základe klasifikácie: High < 1h Medium < 2h Low < 24h
	Coverage	7x24	nonstop prevádzka SOC
Level 2 support	deep analysis	analysis	zhromažďovanie dát súvisiacich s incidentom, pokus o zistenie cesty prieniku a možné následky
		identifications	hľadanie logov a kontrola histórie identifikovaných aktív (PC, server, služba, užívateľ)
	remediation support	communications	poskytnutie správy o incidente zákazníkovi s odporúčaným riešením, podľa zodpovednosti definovaných v RACI
		Isolation	odporučenie najvhodnejšej metódy pre izoláciu problému, alebo priamo izolácia problému podľa pridelených oprávnení
		Remediaton	súčinnosti pri odstraňovaní incidentu
		Documentation	zdokumentovanie priebehu incidentu s poskytnutím odporúčaní, ako predísť opakovaniu
Level 3 support	Post Incident -	Forensic Analysis	digitálna forenzná analýza, zber potrebných doplnkových artefaktov, simulácia v izolovanom prostredí
		Recommendations	na základe odporúčaní identifikácia riešenia a príprava projektu na jeho nasadenie
		Realisation of advisory	implementácia navrhnutých opatrení
		Security Awareness	vysvetlenie jednotlivých krokov pre zákaznícke IT, zdieľanie nadobudnutých vedomostí z incidentu
Level 4 support	Expert escalation	time reservation basic	predplatené hodiny pre expertnú analýzu
			obnova prostredia
			právne poradenstvo
			verejná komunikácia
		time reservation details	Úroveň L4 (Incident Response) v rozsahu 500

	MH (človeko-hodín) vrátane základného posúdenia stavu kybernetickej bezpečnosti v organizácii v rozsahu 100 MH (človeko-hodín)
	identifikácia hrozieb a útočných vektorov relevantných pre organizáciu
	analýza bezpečnostnej architektúry organizácie
	externé posúdenie zraniteľností
	interné posúdenie zraniteľností
	posúdenie konfigurácie core sieťových
	a bezpečnostných prvkov
Escalation requirements	Posúdenie implementovaných bezpečnostných opatrení počas služby bezpečnostného dohľadu s cieľom riešenia incidentu ako pokračovanie eskalácie z L2+ alebo nahlásením incidentu so severitou vysoká až kritická priamo zodpovednou osobou od objednávateľa na kontaktné body poskytovateľa bezpečnostného dohľadu v rozsahu:
	prevzatie hlásenia,
	zber informácií, analýza a hodnotenie incidentu,
	opatrenia na zabránenie ďalšiemu pokračovaniu, šíreniu incidentu (napr. izoláciu napadnutého systému),
	odporúčanie ako zabezpečiť kontinuitu základných služieb,
	odstránenie všetkých nežiadúcich prvkov incidentu a vyčistenie kybernetického prostredia (eradikácia),
	zachytenie digitálnych stôp a forenzná analýza,
	analýza malvéru,
	komunikácia a vyjednávanie s útočníkom v prípade ransomware útoku,
	podpora pri komunikácii s externými subjektmi,
	vypracovanie znaleckého posudku / vypracovanie súdno-znaleckého posudku.
Recovery expectations	určenie stratégie obnovy: spôsob obnovy a časový interval, v rámci ktorého má byť obnova realizovaná, riziká alebo nedostatky, ktoré by mohli kompromitovať efektivitu

	zvolenej stratégie obnovy a predpokladané výsledky
	obnova prevádzky na najnižšiu úroveň poskytovania základných služieb a prechod do normálnej prevádzky
Post-Incident Activities	návrh opatrení na zabránenie opakovaniu výskytu kybernetických bezpečnostných incidentov
Coordination and support	tímov obnovy objednávateľa a dodávateľa služby podpora pri riešení incidentu
	tímov dodávateľov sietí a informačných systémov
	tímov kľúčových používateľov
	komunikácie s dotknutými autoritami
	ďalších nešpecifikovaných účastníkov
SLA	príjem a potvrdenie hlásenia z L3+ je do 10 minút alebo od objednávateľa mimo služby bezpečnostného dohľadu služby je do 30 min. (vzdialená podpora do 12h, podpora na mieste do 24 hodín
	čas na potvrdenie prijatia hlásenia z L3+– do 30 min (T-0)
	čas na triáž hlásenia – do 4 h po prijatí hlásenia (T-4o)
	čas na začatie vzdialenej (remote) asistencie – do 12 h po prijatí hlásenia (T-12o)
	čas na začatie asistencie na mieste (on-site) – do 20 h od rozhodnutia objednávateľa (T-20r)
	as na začatie asistencie na mieste (on-site) - do 24 h od rozhodnutia objednávateľa o zásahu na mieste vykoná počiatočný krok riešenia (T-24r)
	v prípade potreby ďalšieho riešenia dôjde k eskalácii na dodávateľsko - odberateľský reťazec, v prípade podozrenia na spáchaný trestný čin asistovane na žiadosť objednávateľa na orgány činné v trestnom konaní a bude poskytnutá súčinnosť na nahlásenie incidentu na príslušný orgán (autoritu) v zákonom (69/2018) stanovených lehotách
incident report	Ak nie je dohodnuté inak, najneskôr do 10 pracovných

dní po vypracovaní znaleckého posudku (pokiaľ ho objednávateľ písomne vyžiada) dôjde k vypracovaniu vyhodnotenia zásahu vo forme záverečnej správy, ktorá musí obsahovať najmä:

určenie príčin vzniku kybernetického bezpečnostného incidentu a detailný časový priebehu,

zoznam zistených nedostatkov v implementovaných bezpečnostných opatreniach,

odporúčania bezpečnostných opatrení zamedzujúcich opakovanému výskytu kybernetického bezpečnostného incidentu.

8.1.1 Úrovne podpory používateľov

Nemení sa primárna ochrana na žiadnej úrovni, preto nedochádza k zmene v zabehnutých procesoch. Partnerské strany sú určené pre realizáciu projektu a následný začiatok monitorovania: interné IT oddelenie a primárny dodávateľ SOC. Tento dodávateľ SOC zabezpečuje inštaláciu, konfiguráciu a dohľad nad všetkými nástrojmi ako aj odstraňovanie bezpečnostných hrozieb a ich následkov.

SOC team by mal byt rozdelený na viacero úrovní, pričom jednotlivé celky by mali zabezpečovať:

- Monitorovanie a detekcia: Neustále sledovanie IT prostredia (siete, aplikácií, koncových bodov) na identifikáciu podozrivých aktivít a anomálií.
- Analýza a reakcia na incidenty: Rýchla analýza bezpečnostných udalostí a koordinovaná reakcia na zmiernenie dopadov, vrátane forenznej analýzy a nápravy.
- Správa hrozieb: Využitie dát z Threat Intelligence na proaktívne odhaľovanie nových hrozieb a zraniteľností.
- Automatizácia a orchestrácia: Implementácia SOAR nástrojov na automatizáciu rutinných úloh a urýchlenie reakcií na incidenty. Ako aj integrácia systémov do SIEM
- Súlad a reportovanie: Zabezpečenie súladu s regulačnými požiadavkami (napr. GDPR, ISO 27001) a poskytovanie pravidelných správ o bezpečnostnom stave.

Incident response: Forenzná analýza eskalovaných hrozieb spojená Threat Hunting službami s cieľom objaviť infiltráciu nebezpečného kódu alebo útočníka, s následným odstránením týchto hrozieb a zistenie prieniku do systémov spolu s proaktívnym odporúčaním na odstránenie cesty útoku.

8.1.2 Riešenie incidentov – SLA parametre

Z pohľadu incidentov rozlišujeme:

- incidenty na bezpečnostných technológiách samotných.
- incidenty zachytené a vyhodnotené bezpečnostnými nástrojmi (bezpečnostné incidenty)

V oboch prípadoch sú požiadavky na SLA pre bezpečnostné nástroje ako aj SLA pre služby špecifikované detilne v dokumente Opis Predmetu Zákazky

8.2 Požadovaná dostupnosť IS:

V rámci navrhovaného projektu sa nepredpokladá zmena súčasných výkonnostných požiadaviek a požiadaviek na dostupnosť, zálohovanie a obnovu prevádzkovaných ISVS v správe obstarávateľa.

8.2.1 Dostupnosť (Availability)

Nemeníme funkcionalitu kritických aplikácií, pridávame dohľadové technológie. Požiadavky na dostupnosť služieb sú definované v opise predmetu zákazky v jednotlivých funkčných a nefunkčných požiadavkách.

8.2.2 RTO (Recovery Time Objective)

Existujúca technológia a procesy nie sú dotknuté týmto projektom.

8.2.3 RPO (Recovery Point Objective)

Existujúca technológia a procesy nie sú dotknuté týmto projektom.

9. Požiadavky na personál

Personál na dodávku služieb, ich správu a ich použitie je predmetom obstarávania. Neuvažuje sa o zmene v interných zdrojoch pre riadenie ani prevádzku.

10. Implementácia a preberanie výstupov projektu

Realizácia projektu bude formou rámcovej zmluvy, ktorá bude presne špecifikovať podmienky pre prebratie funkčných celkov do prevádzky.

Organizácia projektu a následná prevádzka bude zabezpečovaná nasledovne:

- Interne - Vecný výkon činností kybernetickej bezpečnosti - Odbor kybernetickej bezpečnosti
- Interne - Prevádzka komponentov kybernetickej bezpečnosti – Oddelenie prevádzky IT systémov
- Externe – Prevádzka komponentov kybernetickej bezpečnosti – dodávateľ v zmysle SLA pravidiel

Súčasťou výstupov projektu budú špecializované a manažérske dokumenty v zmysle Vyhlášky č.401/2023

11. Prílohy

Príloha č. 1 – Katalóg požiadaviek

Príloha č. 2 – Register rizík