*Príloha č. 1 Zmluvy o dodaní diela a poskytovaní expertných služieb v oblasti kybernetickej bezpečnosti (ďalej len „**Zmluva**“)*

# OPIS PREDMETU ZÁKAZKY

**NÁZOV ZÁKAZKY: Rozvoj kybernetickej bezpečnosti v ZZS Bratislava**

# Kapitola 1. PREDMET VEREJNÉHO OBSTARÁVANIA

Účelom verejného obstarávania je realizácia cieľov a projektových aktivít IT projektu *„Rozvoj kybernetickej bezpečnosti v ZZS Bratislava*“, kód MetaIS: Projekt_2784, (ďalej aj ako „**IT projekt**“). Záchranná zdravotná služba Bratislava (ďalej ako „**ZZS Bratislava**“ alebo „**verejný obstarávateľ**“) prostredníctvom predloženej zákazky realizuje IT projekt. Podkladom pre vypracovanie Opisu predmetu zákazky bola projektová dokumentácia pre IT projekt, zverejnená v Centrálnom metainformačnom systéme verejnej správy, ktorá má bližšie upravuje ciele, kontext a pre túto zákazku má podporný charakter.

Hlavným cieľom IT projektu je prevencia pred kybernetickými bezpečnostnými incidentmi a zvýšenie miery súladu ZZS Bratislava s požiadavkami všeobecne platných právnych predpisov, najmä:

- zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „**zákon o KB**“),
- zákona č. 95/2018 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „**zákon o ITVS**“),
- zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

a vykonávacími predpismi k vyššie uvedeným zákonom.

Predmetom verejného obstarávania je dodanie diela, ktoré predstavuje funkčný celok, ktorý pozostáva z výstupov, služieb a bezpečnostných nástrojov špecifikovaných v Kapitole 2. OPIS PREDMETU ZÁKAZKY, ich implementácie, konfigurácie a vzájomnej integrácie vrátane zosúladenia ich prevádzky s ďalšími prevádzkovými bezpečnostnými nástrojmi (min. XDR riešenie zn. ESET, DLP riešenie zn. Safetica) (ďalej ako „**dielo**“), za účelom implementácie bezpečnostných opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti vrátane zlepšenia schopnosti detekcie kybernetických bezpečnostných incidentov a v súlade so všeobecne platnými právnymi predpismi tak, ako je definované v tomto dokumente a prílohách, na ktoré sa tento dokument odvoláva.

ZZS Bratislava je tzv. prevádzkovateľ základnej služby podľa zákona o KB, z čoho vyplýva, že verejný obstarávateľ je povinný periodicky overovať úroveň kybernetickej bezpečnosti prostredníctvom nezávislého auditu kybernetickej bezpečnosti. Verejný obstarávateľ oznamuje, že v minulosti vykonal tzv. samohodnotenie, audit kybernetickej bezpečnosti aj inventarizáciu, klasifikáciu a kategorizáciu IT aktív vrátane analýzy rizík kybernetickej bezpečnosti v súlade s platnými právnymi predpismi a metodickými usmerneniami Národného bezpečnostného úradu, ktoré je v súčasnosti potrebné z dôvodu zmien aktualizovať, prepracovať a doplniť.

Verejný obstarávateľ v súčasnosti disponuje základnou organizačnou a riadiacou dokumentáciou pre oblasť informačnej a kybernetickej bezpečnosti (ďalej aj ako „**IKB**“), ktorú je v súčasnosti potrebné z dôvodu zmien aktualizovať, prepracovať a doplniť v rozsahu definovanom v Kapitole 2 tohto dokumentu.

ZZS Bratislava je správcom informačných systémov, ktoré zabezpečujú prevádzku organizácie a poskytovanie zdravotnej starostlivosti pacientom. Patrí medzi ne aj interný agendový systém, ktorý je nemocničný systém s modulmi Doprava a Ústavná lekáreň. Medzi najdôležitejšie funkcionality tohto systému patrí zaznamenávanie výjazdov, spracovanie dávok pre zdravotné poistenie, manažment

spotreby a objednávok liekov a špeciálnych zdravotníckych materiálov. ZZS Bratislava prevádzkuje spolu 94 staníc záchrannej zdravotnej služby (stacionárne pracoviská) rôzneho druhu v rámci Banskobystrického, Bratislavského, Nitrianskeho, Trenčianskeho, Trnavského a Žilinského kraja. Ide o stanice rýchlej zdravotnej pomoci, rýchlej lekárskej pomoci a stanice RZP-S. Počet 94 staníc v súčasnosti zodpovedá približne 65 fyzickým lokalitám, v ktorých je prevádzkovaná IT infraštruktúra verejného obstarávateľa (pozn. uvedené hodnoty sú uvádzané informatívne ako nezáväzný počet a môžu sa meniť v závislosti od organizačných zmien). Ročne zabezpečuje viac než 160 000 výjazdov.

Verejný obstarávateľ si vyhradzuje právo požadovať od dodávateľa aj ďalšiu súčinnosť, ak to bude vyplývať z uzatvorenej Zmluvy o poskytnutí nenávratného finančného príspevku medzi ZZS Bratislava a Ministerstvom investícií, regionálneho rozvoja a informatizácie SR (dostupná na https://www.crz.gov.sk/zmluva/10121328/) a riadiacej dokumentácie pre Program Slovensko vzťahujúcej sa na Cieľ 1, z ktorého je IT projekt financovaný a ktorou je verejný obstarávateľ viazaný. Úspešný uchádzač je povinný tieto požiadavky na súčinnosť splniť v súlade s podmienkami určenými v tejto riadiacej dokumentácii.

# Kapitola 2. OPIS PREDMETU ZÁKAZKY

Predmet zákazky sa skladá z troch logických celkov (na účely tohto dokumentu ďalej aj ako „**modulov**“), ktoré sa ďalej delia na jednotlivé projektové aktivity s príslušným číslovaním projektových aktivít (výstupov). Ide o nasledujúce moduly:

1. Riadenie kybernetickej bezpečnosti
2. Sieťová bezpečnosť a ochrana perimetra
3. Ochrana kritických serverov a bezpečnostný monitoring

Súčasťou každej z častí je dodanie jedného alebo viacerých bezpečnostných nástrojov (licencií) a analytických, implementačných a podporných služieb tak ako sú definované ďalej v tomto dokumente alebo Prílohe č. 2 Zmluvy Špecifikácia požiadaviek. Predmet zákazky sa vzťahuje výlučne na informačné aktíva a IT infraštruktúru v správe (prevádzke) ZZS Bratislava. Verejný obstarávateľ požaduje dodanie všetkých uvedených výstupov minimálne v rozsahu a spôsobom, ktoré sú definované v Zmluve, tomto dokumente a Prílohe č. 2 Zmluvy Špecifikácia požiadaviek.

Verejný obstarávateľ **požaduje dodanie nasledujúcich výstupov**, ktoré sú rozčlenené podľa jednotlivých modulov:

## Modul č. 1: RIADENIE KYBERNETICKEJ BEZPEČNOSTI

### 1.1 Posúdenie súladu s bezpečnostnými požiadavkami

Dodávateľ zabezpečí vykonanie komplexného a detailného posúdenia súladu organizácie s legislatívnymi požiadavkami podľa zákona o KB a súvisiacich vykonávacích predpisov. Posúdenie musí byť vykonané s odbornou starostlivosťou a zahŕňať posúdenie implementovaných bezpečnostných opatrení minimálne na úrovni podľa zákona o KB a jeho vykonávacích predpisov v znení účinnom v čase realizácie. V rámci posúdenia dodávateľ vykoná posúdenie (analýzu) existujúcich bezpečnostných opatrení a ich dostatočnosti s ohľadom na riziká a hrozby kybernetickej bezpečnosti, identifikuje rozdiely medzi aktuálnym stavom a požiadavkami legislatívy (zákon o KB a jeho vykonávacie predpisy), vyhodnotí úroveň implementácie každého z bezpečnostných opatrení a vypracuje konkrétne odporúčania na nápravu zistených nedostatkov, resp. nesúladu s požiadavkami legislatívy.

Zoznam výstupov pre aktivitu 1.1:

a. kontrolný zoznam plnenia všetkých relevantných požiadaviek podľa zákona o KB a vykonávacích predpisov, ich súladu s aktuálnym stavom IKB v ZZS Bratislava, vrátane overenia skutočne implementovaných bezpečnostných opatrení,
b. súbor odporúčaní na zvýšenie účinnosti prijatých bezpečnostných opatrení a odstránenie zistených nesúladov alebo nedostatkov a
c. sumárna hodnotiaca správa o stave IKB v ZZS Bratislava.

### 1.2 Spracovanie základnej dokumentácie pre organizáciu a riadenie IKB

Dodávateľ zabezpečí spracovanie základnej dokumentácie pre organizáciu a riadenie IKB v ZZS Bratislava. Výstupy musia vychádzať z aktuálneho stavu ZZS Bratislava, pričom sa musia zakladať minimálne na aktuálnej organizačnej štruktúre verejného obstarávateľa a rozdelenia jednotlivých úloh a kompetencií, interných riadiacich predpisoch vrátane existujúcich smerníc týkajúcich sa oblasti riadenia IKB a vykonávaných činnostiach ako aj zodpovedať prevádzkovanej IT infraštruktúre. Dodávateľ za účelom dodania nižšie uvedených výstupov realizuje individuálne stretnutia so všetkými identifikovanými vlastníkmi (gestormi) IT aktív, resp. osobami zodpovedajúcimi za IT riziká.

Výstupy musia pokrývať všetky relevantné požiadavky zákona o KB a jeho vykonávacích predpisov účinných v čase realizácie a byť v súlade s metodickými usmerneniami Národného bezpečnostného úradu a Ministerstva investícií, regionálneho rozvoja a informatizácie SR. Ak takých metodických usmernení niet, tak výstupy musia byť v súlade s medzinárodnými štandardmi radu ISO 27000 a príkladmi najlepšej praxe (tzv. best practices).

Zoznam výstupov pre aktivitu 1.2:

a. aktualizovaný zoznam identifikovaných informačných aktív ZZS Bratislava s ich kompletnou evidenciou na úrovni minimálne presnej identifikácie IT aktíva, popisu, podporného aktíva, druhu, vlastníka/správcu,
b. aktualizovaná, doplnená a prepracovaná inventarizácia a klasifikácia informácií,
c. aktualizácia analýzy rizík kybernetickej bezpečnosti a analýzy dopadov (AR/BIA), ktorá je založená na Metodike analýzy rizík kybernetickej bezpečnosti, verzia 2.0 alebo novšia, vydanej Národným bezpečnostným úradom (ďalej ako „**NBÚ**“) dňa 01. septembra 2025, a ktorá je plne v súlade s medzinárodným štandardom ISO 27005. Analýza rizík kybernetickej bezpečnosti vykonaná podľa tejto metodiky je založená na semikvantitatívnej analýze. Výstup zahŕňa prepracovanie a doplnenie uvedených dokumentov, revíziu a zreálnenie ohodnotenia a vlastníkov rizík, opatrení na zníženie rizika, relevantných kybernetických hrozieb a vytvorenie aktuálneho katalógu hrozieb, ktorý sa odvíja od vzorov NBÚ, katalógu zraniteľností a spolu s revíziou a zreálnením zraniteľností. Súčasťou odovzdanej analýzy rizík je najmä sumárna hodnotiaca správa, ktorá obsahuje najmenej manažérske zhrnutie, informáciu o použitej metodike a opis postupov, kľúčové zistenia/odporúčania na zvýšenie úrovne kybernetickej bezpečnosti, vlastnú analýzu rizík a analýzu dopadov (AR/BIA), prehľad aktív, hrozieb, prehľad všetkých rizík (nových, zmenených, nezmenených), návrh plánu ošetrenia rizík, záver.
d. Spracovanie smerníc a prevádzkovej dokumentácie pre organizáciu a riadenie IKB, minimálne v nasl. rozsahu:
    - Stratégia kybernetickej bezpečnosti
      Definuje jednoznačné a merateľné strategické ciele, pričom po ich naplnení bude možné zhodnotiť ich dopad na zlepšenie systému informačnej a kybernetickej bezpečnosti. Výstupom bude dokument definujúci požiadavky a ciele na strategickej úrovni v oblasti informačnej a kybernetickej bezpečnosti. Predmetná stratégia musí spĺňať štruktúru a byť v súlade s obsahovými požiadavkami podľa vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej ako „**vyhláška č. 227/2025 Z. z.**“)
    - Bezpečnostná politika
      Predstavuje základný a nadradený dokument systému riadenia informačnej bezpečnosti organizácie. Definuje strategický rámec, ciele a princípy ochrany

informačných aktív, ako aj zodpovednosti a povinnosti všetkých zainteresovaných strán. Cieľom bezpečnostnej politiky je stanoviť jednotný prístup k zabezpečeniu dôvernosti, integrity, dostupnosti a odolnosti informačných systémov a informácií, pričom zohľadňuje požiadavky zákona o KB a jeho vykonávacích predpisov

- Bezpečnostná smernica pre používateľov
  Stanovuje pravidlá a zásady správania všetkých používateľov informačných a komunikačných technológií ZZS Bratislava. Jej cieľom je zabezpečiť zodpovedné, bezpečné používanie systémov, zariadení a sietí v súlade s požiadavkami zákona o KB a jeho vykonávacích predpisov, pričom sa riadi princípmi ochrany dôvernosti, integrity a dostupnosti informácií.

- Smernica o bezpečnej prevádzke IS pre správcov IT
  Určuje pravidlá a povinnosti pre správcov IT a technický personál zodpovedný za správu, údržbu a bezpečnosť informačných systémov ZZS Bratislava. Jej cieľom je zabezpečiť stabilnú, spoľahlivú a bezpečnú prevádzku systémov, ktoré podporujú kľúčové procesy ZZS Bratislava.

- Smernica pre riadenie informačnej bezpečnosti
  Predstavuje základný rámec pre zavedenie, udržiavanie a zlepšovanie systému riadenia informačnej bezpečnosti (ISMS) v organizácii. Jej cieľom je zabezpečiť primeranú ochranu informačných aktív pred stratou, neoprávneným prístupom, zneužitím, poškodením alebo narušením dostupnosti

- Smernica pre riadenie aktív a rizík, vrátane AR/BIA metodiky vytvorenej v súlade s metodikou NBÚ a prispôsobenej podmienkam verejného obstarávateľa
  Stanovuje systematický prístup k identifikácii, evidencii, klasifikácii a ochrane informačných aktív, ako aj k riadeniu bezpečnostných rizík, ktoré môžu ohroziť dôvernosť, integritu, dostupnosť alebo funkčnosť týchto aktív. Dokument je vypracovaný v súlade s požiadavkami zákona o KB a jeho vykonávacími predpismi, ako aj v súlade s metodikou pre analýzu rizík a BIA (Business Impact Analysis) odporúčanou NBÚ a prispôsobenou potrebám verejného obstarávateľa.

- Smernica o klasifikácii informácií
  Vypracovaná podľa klasifikačnej schémy definovanej v zákone o KB a jeho vykonávacích predpisoch vrátane adaptácie pre potreby verejného obstarávateľa.

- Smernica riadenia prístupových práv
  Upravuje pravidlá a mechanizmy riadenia prístupových práv k informačným systémom, sieťam a informáciám ZZS Bratislava. Cieľom smernice je zabezpečiť, aby prístup k citlivým, dôverným a prevádzkovo kritickým informáciám mali len oprávnené osoby, a to v rozsahu nevyhnutnom na plnenie ich pracovných úloh.

- Smernica pre riadenie dodávateľských služieb a tretích strán
  Stanovuje pravidlá a požiadavky pre bezpečné riadenie vzťahov s dodávateľmi a tretími stranami, ktorí poskytujú služby, prístup k informačným systémom, informáciám, priestorom alebo iným aktívam ZZS Bratislava. Cieľom smernice je zabezpečiť, aby služby poskytované externými subjektmi neohrozovali bezpečnostnú politiku organizácie a aby boli primerane chránené informačné aktíva, ku ktorým môžu mať dodávatelia prístup.

- Smernica ohľadom bezpečnostných požiadaviek pre obstarávanie nových IS (SSDLC)

Upravuje koncept životného cyklu vývoja systémov, ktorý sa vzťahuje na HW a SW konfigurácie. Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek.

(*) Verejný obstarávateľ si vyhradzuje právo navrhnúť nahradenie niektorého z výstupov uvedených v bode 1.2 písm. d) za inú smernicu s obdobnou prácnosťou, ak takáto požiadavka bude vyplývať v budúcnosti z vykonaného nezávislého auditu kybernetickej bezpečnosti, o čom s dostatočným predstihom upovedomí dodávateľa, skonzultujú odhad prácnosti a v prípade súhlasu oboch zmluvných strán spíšu o takejto dohode protokol.

1.3 Dodanie nástroja na procesno-organizačné riadenie IKB (ďalej ako „**bezpečnostný nástroj 1**“)

Predmetom je dodanie licencie pre bezpečnostný nástroj 1, ktorého funkčné požiadavky sú definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek, a inštalačné a konfiguračné práce pre tento nástroj. Implementácia bezpečnostného nástroja 1 zahŕňa jeho:

a. uvedenie do prevádzky, nastavenie manažmentu prístupov, nastavenie centrálnej konzoly pre používateľov podľa dostupných možností a požiadaviek verejného obstarávateľa;
b. nastavenie a vloženie všetkých relevantných informácií o verejnom obstarávateľovi, vrátane vloženia (evidencie) alebo priamo v rámci bezpečnostného nástroja 1 vypracovania výstupov definovaných v aktivitách vyššie (minimálne Kapitola 2, bod 1.2) do bezpečnostného nástroja 1,
c. ďalšia konfigurácia, plné sprevádzkovanie a vloženie aktuálnych dát v spolupráci s verejným obstarávateľom minimálne v rozsahu jednotlivých funkcionalít definovaných v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Bezpečnostný nástroj 1).

Zoznam výstupov pre aktivitu 1.3:

a. plne funkčný a do riadnej prevádzky uvedený bezpečnostný nástroj 1, ktorý poskytuje plnú funkcionalitu a spĺňa minimálne požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek.

1.4 Realizácia bezpečnostných testovaní a skenovaní zraniteľností

Verejný obstarávateľ požaduje dodanie (A) bezpečnostných testovaní zamestnancov ZZS Bratislava a (B) realizáciu skenov zraniteľností (tzv. vulnerability scan).

**(A)** Verejný obstarávateľ požaduje realizovať bezpečnostné testovanie zamestnancov ZZS Bratislava formou tzv. spear phishingového testu za pomoci simulačnej platformy, do ktorej bude mať počas testovania prístup aj verejný obstarávateľ. Tento test bude zameraný na overenie schopnosti zamestnancov verejného obstarávateľa rozpoznať pokročilý phishingový útok a bude simulovať skutočné útoky tohto typu.

Každý test musí mať vytvorený unikátny scenár, tzn. bude individualizovaný pre prostredie verejného obstarávateľa alebo prispôsobený pre rôzne skupiny používateľov s účelom sťažiť jeho rozpoznanie prostredníctvom prispôsobenia vzhľadu a obsahu e-mailovej správy a cieľovej internetovej stránky a realizovaný podľa podmienok, pravidiel a v čase (testovacom okne), ktoré schvaľuje verejný obstarávateľ. Charakter testu (scenár) musí umožniť rozlíšiť jednotlivých používateľov verejného

obstarávateľa podľa aktivity, ktorú vykonali alebo nevykonali. Bezpečnostné testovanie musí podporovať nasledujúce technicky testovania zamestnancov: (1) E-mailová správa, ktorá bude používateľa nabádať na jednu z akcií: kliknutie na odkaz, odpoveď na e-mail, otvorenie prílohy, a (2) Cieľová internetová stránka, na ktorej bude umiestnený obsah nabádajúci používateľa na jednu z akcií: kliknutie na odkaz, vloženie prihlasovacích údajov alebo iných údajov, stiahnutie súboru.

Verejný obstarávateľ sa zaväzuje poskytnúť dodávateľovi minimálnu potrebnú súčinnosť pre umožnenie realizácie bezpečnostného testovania, a to minimálne verifikáciu simulačnej platformy voči IT systémom ZZS Bratislava s cieľom zabezpečiť čo najvyššiu mieru doručiteľnosti e-mailových správ zamestnancom verejného obstarávateľa.

**(B)** Verejný obstarávateľ požaduje realizovať sken zraniteľností formou externého a interného skenovania IT infraštruktúry ZZS Bratislava. Zahŕňa skenovanie zraniteľností rozsahu IP adries dostupných zo siete internet a skenovanie systémov, pracovných staníc a sieťovej infraštruktúry verejného obstarávateľa, ktoré sú dostupné z vnútornej siete. Sken zraniteľností bude realizovaný podľa podmienok, pravidiel a v čase, ktoré navrhuje dodávateľ a ktoré následne podlieha schváleniu verejného obstarávateľa.

Detailné informácie k realizácii bezpečnostných testovaní a skenovaní zraniteľností sú uvedené v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Skenovanie zraniteľností).

Zoznam výstupov pre aktivitu 1.4:

a. realizované bezpečnostné testovania zamestnancov verejného obstarávateľa, minimálne v počte 4. Výstup zahŕňa správu o výsledku každého z realizovaných testovaní (protokol), ktorý obsahuje prehľadne uvedené informácie podľa toho, či príjemca:
    - predmetný e-mail dostal,
    - e-mail otvoril,
    - otvoril internetový odkaz v e-maili,
    - otvoril súbor v prílohe e-mailu,
    - na e-mail odpovedal,
    - vyplnil a odoslal požadované údaje na cieľovej webovej stránke,
    - nahlásil phishingový útok podľa interného postupu,
b. skenovania zraniteľností, minimálne v počte 4 s časovým odstupom medzi jednotlivými skenovaniami dohodnutým s verejným obstarávateľom. Súčasťou je odovzdanie a prezentácia záverečnej správy o výsledku každého z realizovaných testovaní (protokol), ktorá obsahuje manažérske zhrnutie s vyhodnotením testu, základné údaje minimálne o rozsahu, cieľoch a zameraní testovania, použitej metodológii alebo postupe, využitých technických nástrojoch, výsledkoch testovania a odporúčaniach na zavedenie nápravných opatrení, ak je to potrebné. Súčasťou výstupu je aj odovzdanie zdrojových (raw) dát z testu. Detailné požiadavky na reporting výsledkov skenovaní zraniteľností sú uvedené v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Skenovanie zraniteľností).

**Modul č. 2: SIEŤOVÁ BEZPEČNOSŤ A OCHRANA PERIMETRA**

2.1 Dodanie a implementácia nástroja pre ochranu perimetra (NGFW) (ďalej ako „**bezpečnostný nástroj 2**“)

Výstupom je dodanie a inštalácia 2 ks HW zariadení bezpečnostného riešenia s príslušnou licenciou pre ochranu perimetra verejného obstarávateľa za účelom správy sieťovej prevádzky a blokovania nebezpečnej sieťovej komunikácie, ktoré spĺňa požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Bezpečnostný nástroj 2). Verejný obstarávateľ požaduje dodanie bezpečnostného nástroja 2 realizovať ako náhradu pôvodného firewallu zn. Cisco.

V rámci implementačných prác pre bezpečnostný nástroj 2 verejný obstarávateľ požaduje vykonanie všetkých úkonov, ktoré sú potrebné na uvedenie bezpečnostného nástroja 2 do riadnej prevádzky v zmysle dostupných funkcionalít, aplikovateľných bezpečnostných politík a odporúčaných pracovných postupov výrobcu uchádzačom ponúkaného technologického riešenia. Rozsah prác zahŕňa najmenej tieto postupy, resp. požiadavky (pozn. poradie uvedených postupov/požiadaviek je indikatívne):

a. Analýza a posúdenie aktuálne prevádzkovaného firewallu zn. Cisco:
    i. detailná evidencia a revízia existujúcej konfigurácie na úrovni pravidiel firewallu, pravidlá NAT (Network Address Translation), VPN konfigurácie (site-to-site, remote access) a politiky prístupu (Access Control Lists).
    ii. Evidencia existujúcich pravidiel a politík firewallu, aktuálneho nastavenia sieťovej segmentácie a ostatných konfigurácií. Zahŕňa aj validáciu a audit bezpečnostných politík a jednotlivých existujúcich pravidiel, identifikáciu nevyužívaných alebo redundantných pravidiel, ktoré je možné odstrániť alebo upraviť pre efektívnejšiu implementáciu v bezpečnostnom nástroji 2, a prehodnotenie stavu súčasných bezpečnostných opatrení, ako sú IPS/IDS, URL filtering, aplikácia opatrení pre tzv. Quality of Service (QoS) a analýza ich efektivity.
    iii. Verejný obstarávateľ požaduje v rámci tejto fázy vypracovať aj plán prác, ktorý bude zahŕňať opis realizovaných technologických postupov.
    iv. Posúdenie závislostí: Zmapovanie všetkých zariadení a aplikácií závislých na existujúcich firewall pravidlách (napr. serverov, databáz, interných služieb) a testovanie konektivity so sieťovými zariadeniami verejného obstarávateľa. Určenie požiadaviek na šírku pásma (bandwidth) a dostupnosť pri prechode na nové riešenie. Preverenie potreby zachovania súčasného VPN pripojenia (ak je aplikované) medzi jednotlivými pobočkami alebo remote users, a zabezpečenie kompatibility s NGFW.
b. Dizajn a návrh architektúry pre implementáciu bezpečnostného nástroja 2, fyzického a logického zapojenia.
c. Prechod a migrácia z existujúceho na nové riešenie:
    i. Určiť vhodný harmonogram a časové okno pre migráciu s ohľadom na minimalizovanie výpadkov alebo obmedzenie dostupnosti služieb pre používateľov ZZS Bratislava.
    ii. Implementovať nové riešenie počas tzv. prechodnej fázy (transition period) pre minimalizáciu rizika obmedzenia dostupnosti služieb pre používateľov ZZS Bratislava, a teda jeho zavádzanie v paralelnom režime so starým systémom, aby sa v prípade neúspechu migrácie mohli aplikovať okamžité nápravné opatrenia. Počas tejto fázy

verejný obstarávateľ požaduje monitorovať stabilitu, výkonnosť, dostupnosť služieb a overovať, či sú bezpečnostné pravidlá správne aplikované.

iii. Migrácia existujúcich bezpečnostných pravidiel firewallu, politík a konfigurácií (napr. NAT pravidlá, VPN konfigurácie, prístupové politiky a pod.), konfigurácia a testovanie kompatibility s existujúcimi sieťovými zariadeniami a aplikáciami.

iv. V rámci tzv. prechodnej fázy je potrebné zabezpečiť vyladenie a otestovanie každej z požadovaných funkcionalít do funkčného stavu.

v. Verejný obstarávateľ požaduje aktiváciu a konfiguráciu všetkých dostupných a zároveň aplikovateľných funkcionalít definovaných v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Bezpečnostný nástroj 2) so zohľadnením rizík kybernetickej bezpečnosti, ak sa zmluvné strany nedohodnú inak.

vi. Odpojenie existujúceho firewallu zn. Cisco.

d. Záverečné testovanie a validácia nastavení a konfigurácií bezpečnostného nástroja 2 v produkčnej prevádzke.

Verejný obstarávateľ požaduje na vykonanie všetkých potrebných prác súvisiacich s implementáciou bezpečnostného nástroja 2 časovú alokáciu odborných zamestnancov dodávateľa súhrnne v minimálnom rozsahu 6 človekodní (1 človekodeň = 8 hodín).

Zoznam výstupov pre aktivitu 2.1:

a. plne funkčný a do riadnej prevádzky uvedený bezpečnostný nástroj 2, ktorý poskytuje plnú funkcionalitu a spĺňa minimálne požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek.

**Modul č. 3: OCHRANA KRITICKÝCH SYSTÉMOV A BEZPEČNOSTNÝ MONITORING**

3.1 Dodanie a implementácia nástroja pre ochranu kritických serverov (ďalej ako „**bezpečnostný nástroj 3**“)

Predmetom implementácie je zavedenie komplexného bezpečnostného riešenia pre ochranu kritických infraštruktúrnych prvkov (serverov), ktoré spĺňa požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Bezpečnostný nástroj 3) vrátane funkcionality „virtual patching“ pre tzv. legacy systémy, pre ktoré už nie sú vydávané bezpečnostné záplaty, a ochrany pred zneužitím (exploitáciou) tzv. zero-day zraniteľností.

Verejný obstarávateľ požaduje nasadenie bezpečnostného nástroja 3 na serverovej infraštruktúre ZZS Bratislava. Verejný obstarávateľ požaduje vykonanie všetkých nevyhnutných implementačných, konfiguračných a testovacích úkonov, ktoré sú potrebné na uvedenie bezpečnostného nástroja 3 do riadnej prevádzky v zmysle dostupných funkcionalít, aplikovateľných bezpečnostných politík, zohľadnením rizík kybernetickej bezpečnosti a odporúčaných pracovných postupov výrobcu uchádzačom ponúkaného technologického riešenia. Rozsah prác zahŕňa najmenej tieto postupy, resp. požiadavky (pozn. poradie uvedených postupov/požiadaviek je indikatívne):

a. Analýza infraštruktúry a posúdenie závislostí: Zmapovanie všetkých zariadení a aplikácií závislých na serverovej infraštruktúre. Súčasťou je identifikácia rizík spojených s implementáciou a posúdenie dopadu na prevádzkové procesy. Verejný obstarávateľ

požaduje v rámci tejto fázy vypracovanie plánu prác s uvedením postupu pre implementáciu bezpečnostného nástroja 3.

b. Inštalácia a konfigurácia agenta: nasadenie agenta na operačných systémoch, konfigurácia agenta musí zahŕňať nastavenie autentifikácie, šifrovanej komunikácie s manažment konzolou, politiky nasadzovania aktualizácií (tzv. virtual patching), pravidiel pre detekciu a blokovanie podozrivých aktivít, logovania a správy alertov a konfiguráciu dostupných bezpečnostných funkcionalít (politík) bezpečnostného nástroja 3.
c. Testovanie: Testovanie musí zahŕňať validáciu detekčných a blokovacích mechanizmov pre jednotlivé bezpečnostné moduly (antimalware, firewall, IDS/IPS, virtual patching atď.), simuláciu škodlivých aktivít v monitorovanom prostredí, vyhodnotenie false positive/false negative miery detekcie a optimalizácia prevádzky (ladenie) s ohľadom na stabilitu a výkon informačných systémov verejného obstarávateľa, funkčnosť detekčných scenárov a minimalizáciu tzv. false positive alertov.

Zoznam výstupov pre aktivitu 3.1:

a. plne funkčný a do riadnej prevádzky uvedený bezpečnostný nástroj 3, ktorý poskytuje plnú funkcionalitu a spĺňa minimálne požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek.

3.2 Dodanie a implementácia nástroja pre bezpečnostný monitoring (ďalej ako „**bezpečnostný nástroj 4**“)

Predmetom implementácie je zavedenie komplexného bezpečnostného riešenia pre bezpečnostný monitoring infraštruktúry ZZS Bratislava, ktorý spĺňa požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek (časť Bezpečnostný nástroj 4), s integrovaným centrálnym log manažmentom pre účely agentového aj bezagentového zberu a uchovávania logov zo systémov organizácie, sieťových zariadení a koncových staníc s dostatočnou kapacitou pre ukladanie bezpečnostných logov v rámci cloudového úložiska výrobcu navrhovaného bezpečnostného nástroja 4 minimálne po dobu 18 mesiacov.

Verejný obstarávateľ požaduje, aby bol bezpečnostný nástroj 4 prevádzkovaný v cloudovom prostredí výrobcu a disponoval funkcionalitami SIEM a Extended Detection and Response (XDR), Attacker Behavior Analytics (ABA), User Behavior Analytics (UBA), Network Traffic Analysis (NTA), File Access Activity Monitoring (FAAM), File Integrity Monitoring (FIM), Deception Technology pre zabezpečenie komplexného monitoringu infraštruktúry ZZS Bratislava a možnosti vyhodnocovania bezpečnostných udalostí (celý rozsah požiadaviek je uvedený v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek).

Verejný obstarávateľ požaduje nasadenie bezpečnostného nástroja 4 na serverovej infraštruktúre a koncových bodoch ZZS Bratislava, rovnako ako aj integráciu (nastavenie zberu a zasielania aplikačných, databázových alebo systémových logov) s ostatnými zariadeniami ZZS Bratislava (najmä aktívne alebo pasívne sieťové zariadenia verejného obstarávateľa, bezpečnostné nástroje 2 a 3).

Verejný obstarávateľ požaduje vykonanie všetkých nevyhnutných implementačných, konfiguračných a testovacích úkonov, ktoré sú potrebné na uvedenie bezpečnostného nástroja 4 do riadnej prevádzky v zmysle dostupných funkcionalít, aplikovateľných bezpečnostných politík a odporúčaných pracovných postupov výrobcu uchádzačom ponúkaného technologického riešenia. Rozsah prác

zahŕňa najmenej tieto postupy, resp. požiadavky (pozn. poradie uvedených postupov/požiadaviek je indikatívne):

a. Analýza infraštruktúry: Analýza prostredia ZZS Bratislava a zmapovanie všetkých IT zariadení a bezpečnostných technológií verejného obstarávateľa, definovanie rozsahu zdrojov logov (tzv. logsources), ktoré budú zbierané, a technológií, ktoré budú s nástrojom integrované. Táto fáza zahŕňa aj prípravu IT infraštruktúry, na ktorej má byť bezpečnostný nástroj nasadený, v spolupráci s verejným obstarávateľom Verejný obstarávateľ požaduje v rámci tejto fázy vypracovanie plánu prác s uvedením postupu pre implementáciu bezpečnostného nástroja 4.
b. Inštalačné a konfiguračné práce:
    i. Inštalácia agentov na koncových bodoch (servery, pracovné stanice).
    ii. Konfigurácia agentov, korelačných pravidiel (use cases), nastavenie pravidiel pre zasielanie alertov a upozornení,
    iii. Konfigurácia ďalších dostupných bezpečnostných funkcionalít (politík) bezpečnostného nástroja 4 podľa Prílohy č. 2 Špecifikácia požiadaviek.
c. Testovanie: Testovanie musí zahŕňať validáciu funkčnosti detekčných scenárov a korelačných pravidiel, vyhodnotenie false positive/false negative miery detekcie a optimalizácia prevádzky (ladenie) s ohľadom na stabilitu a výkon informačných systémov verejného obstarávateľa, funkčnosť detekčných scenárov a minimalizáciu tzv. false positive alertov.

Zoznam výstupov pre aktivitu 3.2:

a. plne funkčný a do riadnej prevádzky uvedený bezpečnostný nástroj 4, ktorý poskytuje plnú funkcionalitu a spĺňa minimálne požiadavky definované v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek.

3.3 Služby bezpečnostného monitoringu kritických aktív

Zabezpečenie služby bezpečnostného monitoringu SOC as a service pre kritické aktíva verejného obstarávateľa vrátane podpory riešenia bezpečnostných incidentov po dobu trvania projektu. Kritickými aktívami sa rozumie serverová infraštruktúra (virtuálne, fyzické, cloudové servery), ktorá je kľúčová pre zabezpečenie prevádzky základnej služby ZZS Bratislava.

Služba bezpečnostného monitoringu SOC musí napĺňať minimálne nasledovné požiadavky:

a. aktívny a nepretržitý bezpečnostný monitoring v režime 24/7 pomocou bezpečnostných nástrojov implementovaných v rámci IT projektu, ktorý pokrýva dostupné oblasti kybernetickej bezpečnosti podľa zákona o KB a vykonávacích predpisov,
b. nastavenie automatickej notifikácie bezpečnostných udalostí podľa požiadaviek verejného obstarávateľa,
c. detekcia kybernetických bezpečnostných incidentov,
d. evidencia detegovaných bezpečnostných udalostí a incidentov v rámci implementovaných bezpečnostných nástrojov a ich sledovanie,
e. zníženie ich dopadov v reakčných časoch primeraných kategórii incidentu,
f. zdieľanie informácií z databázy zachytených incidentov,

g. spolupráca na priebežnom ladení dátových modelov/korelačných pravidiel v súlade s potrebami monitorovanej infraštruktúry a dostupnosťou potrebných informácií,
h. dopĺňanie korelačných pravidiel v nadväznosti na možnosti monitorovanej technológie a požiadavky verejného obstarávateľa v rozsahu implementovaného riešenia,
i. poskytnutie poradenstva pre zladenie interných procesov riešenia bezpečnostných incidentov (internej smernice) s procesmi SOC

Verejný obstarávateľ požaduje, aby uchádzač poskytoval služby bezpečnostného monitoringu kritických aktív s nasledujúcimi maximálnymi reakčnými časmi odozvy:

a. prvotná reakcia (odozva) na kritický alert: do 1 hodiny,
b. priebežná aktualizácia počas kybernetického bezpečnostného incidentu o stave jeho riešenia: minimálne každých 24 hodín,
c. doručenie mesačného reportu: do 10 pracovných dní nasledujúceho kalendárneho mesiaca.

Služba bezpečnostného monitoringu kritických aktív ďalej zahŕňa služby vyšetrovania a analýzy, ktoré pozostávajú z:

a. IoC Sweeping: Pravidelné prehľadávanie prostredia na základe nových indikátorov kompromitácie (IoC) s cieľom odhaliť doposiaľ nedetegované kybernetické bezpečnostné incidenty.
b. Proaktívny Threat Hunting: Aktívne vyhľadávanie anomálneho správania a skrytých hrozieb, ktoré obchádzajú štandardné detekčné mechanizmy.
c. Analýza príčiny (tzv. RCA): Vytvorenie detailnej časovej osi a popisu kybernetického útoku – vektor, rozsah a dopad kybernetického bezpečnostného incidentu.
d. Analýza dopadu: Zistenie, ktoré ďalšie systémy v prostredí mohli byť kybernetickým bezpečnostným incidentom kompromitované.
e. Prioritizácia incidentov: Posúdenie závažnosti alertov a ich eskalácia podľa definovaných pravidiel a kritickosti aktív.
f. Poskytovanie nevyhnutnej miery súčinnosti príslušným orgánom v prípade závažného kybernetického bezpečnostného incidentu.

Služba bezpečnostného monitoringu kritických aktív ďalej zahŕňa služby reakcie na kybernetické bezpečnostné incidenty a nápravy, ktoré pozostávajú z:

a. Koordinovaná reakcia: Dodanie presného a zrozumiteľného plánu krokov na zastavenie kybernetického útoku a obmedzenie škôd.
b. Odporúčania na nápravu: Poskytnutie odporúčaní na úplné odstránenie hrozby z prostredia a obnovu systémov do bezpečného stavu.
c. Asistencia pri obnove: V prípade potreby poskytnutie špecifických nástrojov (napr. skriptov) na podporu čistenia systémov.

Požiadavky na prevádzku a reporting

a. Mesačné reporty: Pravidelné reporty sumarizujúce bezpečnostné udalosti, vyriešené kybernetické bezpečnostné incidenty, SLA plnenie a strategické odporúčania.

b. Incident report: Detailný report konkrétneho kybernetického bezpečnostného incidentu (základné informácie o incidente, popis incidentu, príčinu incidentu, priebeh reakcie na incident, dôsledky a dopady, nápravné opatrenia, záver a odporúčania).

Zoznam výstupov pre aktivitu 3.3:

a. nastavenie a zavedenie služby a prevádzka proaktívneho bezpečnostného monitoringu (SOC as a service) v zmysle požiadaviek,
b. poskytovanie služieb bezpečnostného monitoringu pre kritické aktíva vrátane služieb vyšetrovania, analýzy a reakcie na kybernetické bezpečnostné incidenty.

# Kapitola 3. ROZSAH ZÁKAZKY A LICENČNÉ PODMIENKY

Zákazka je realizovaná formou zmluvy o dielo, ktorá sa uzatvára na obdobie 17 mesiacov od účinnosti zmluvy.

Požadovaná dĺžka licenčného obdobia pre bezpečnostné nástroje 1 až 4 je 2x12 mesiacov od dátumu aktivácie licencií každého bezpečnostného nástroja. Moment aktivácie každej z licencií určí verejný obstarávateľ.

ZZS Bratislava požaduje nasadenie uvedených bezpečnostných nástrojov a realizáciu aktivít, ktoré sú uvedené v Kapitole 2. Opis predmetu zákazky, pre nasledujúci rozsah:

a. počet agendových informačných systémov: 10,
b. počet interných používateľov: 1200,
c. 180 pracovných staníc (desktopy a notebooky s OS MS Windows 10 alebo MS Windows 11),
d. Windows servery s Microsoft Active Directory a s Hyper-V: spolu 10 fyzických, 20 virtuálnych serverov,
e. počet fyzických adries okrem centrály: 54, na každej adrese je umiestnený 1 router,
f. rozsah IP adries dostupných zo siete internet: 59 (z toho 5 IP adries riaditeľstvo),
g. počet ostatných zariadení: viď tabuľka nižšie:

| | Centrála | Poznámky |
|---|---|---|
| Zdroj udalosti | Počet | Popis zariadenie / OS |
| AD, LDAP, DHCP, DNS... | 2 | |
| Firewall | 1 | |
| Switche a access pointy | 20 | |
| Fyzické servery | 10 | |
| Virtuálne servery | 20 | Virtualizačná platforma: Hyper-V |
| Databázy | 8 | |
| PC / notebook / antivirus | 50 | |
| VPN | 30 | |
| Sieťové tlačiarne | 15 | |
| | Stanice ZZS Bratislava | Poznámky |
| Switche a access pointy | 80 | Z uvedeného počtu je 54 routerov, ktoré patria verejnému obstarávateľovi |
| PC / notebook / antivirus | 130 | |
| VPN | 130 | |
| Sieťové tlačiarne | 10 | |

Uvedenému počtu zariadení, IT systémov a používateľov musí zodpovedať licenčné pokrytie bezpečnostných nástrojov, resp. rozsah dodávaných služieb, ktoré sú definované v Kapitole. Opis predmetu zákazky.

# Kapitola 4. ŠPECIFIKÁCIA IMPLEMENTAČNÝCH A POSTIMPLEMENTAČNÝCH SLUŽIEB

## 4.1 IMPLEMENTAČNÁ FÁZA

Implementačná fáza zahŕňa vypracovanie a dodanie všetkých výstupov a všetky inštalačné a konfiguračné práce definované v Kapitole 2. Opis predmetu zákazky. Implementačná fáza končí zaškolením personálu. Implementačná fáza plynie pre každú projektovú aktivitu a každý výstup nezávisle od ostatných.

Verejný obstarávateľ požaduje pred začiatkom realizácie každej z projektových aktivít vypracovanie **rozvrhu prác**, ktorý zahŕňa opis realizovaných technologických postupov, indikatívne termíny, požiadavky na súčinnosť a závislosti v prípade, že boli identifikované. Rozvrh prác je dodávateľ povinný s verejným obstarávateľom s dostatočným predstihom konzultovať a pred začiatkom realizácie jednotlivých projektových aktivít ho písomne predložiť verejnému obstarávateľovi na schválenie (napr. e-mailom). Dodávateľ a verejný obstarávateľ sú povinní sa počas realizácie zákazky riadiť schváleným detailným rozvrhom prác (termíny uvedené v časti 4.3 Harmonogram tejto kapitoly týmto nie sú dotknuté).

Dodávateľ nesie výhradnú zodpovednosť za výber vhodného technického postupu a realizáciu konkrétnych krokov pri implementácii jednotlivých výstupov, ktoré sú definované v Kapitole 2. Opis predmetu zákazky. Dodávateľ je povinný zvoliť také riešenia, ktoré budú v súlade s aktuálne uznávanými odbornými štandardmi a osvedčenými postupmi (best practices) v oblasti kybernetickej bezpečnosti a IT. Ak dokumentácia neobsahuje konkrétne požiadavky na implementáciu alebo sa zmluvné strany nedohodnú inak, verejný obstarávateľ vyžaduje, aby sa implementačné práce realizovali v súlade s odporúčanými postupmi výrobcov dodávaných technológií a platnými štandardmi, a ak takéto postupy alebo štandardy neexistujú, podľa osvedčenej praxe, pričom dodávateľ zodpovedá za výber a uplatnenie takých riešení a postupov, ktoré zabezpečia najvyššiu možnú úroveň odbornej starostlivosti a ochrany záujmov ZZS Bratislava.

Verejný obstarávateľ požaduje zabezpečiť realizáciu IT projektu minimálne prostredníctvom expertov uvedených v Súťažných podkladoch pre tento predmet zákazky, konkrétne požiadavkách na odbornú spôsobilosť: „**Odborné požiadavky na kľúčových expertov**“. Jednotliví experti musia participovať na aktivitách IT projektu minimálne v rozsahu zodpovedajúcemu odbornej náročnosti. **Dodávateľ je povinný zabezpečiť zapojenie kľúčových expertov v rozsahu určenom verejným obstarávateľom v jednotlivých moduloch.**

Zoznamy implementačných služieb uvedené v tejto zmluve predstavujú minimálny požadovaný rozsah prác a ich poradie je indikatívne. Verejný obstarávateľ si vyhradzuje právo požadovať úpravu alebo doplnenie implementačných činností, pokiaľ to bude nevyhnutné pre funkčnosť diela a v súlade s odbornými štandardmi. Implementačné služby musia prebiehať v súlade s požiadavkami verejného obstarávateľa a ak nie sú, tak po predchádzajúcej konzultácii s ním. Verejný obstarávateľ si vyhradzuje právo požadovať zmenu navrhovaného pracovného postupu, ak to vyplýva z prevádzkových požiadaviek ZZS Bratislava.

Verejný obstarávateľ môže schváliť drobné odchýlky alebo zmeny v navrhovanej technologickej architektúre a inštalačných prácach, ktoré sú definované v tomto dokumente, ak sú tieto úpravy

nevyhnutné z dôvodu špecifických technologických postupov, požiadaviek na funkcionalitu či vzájomnú kompatibilitu informačných systémov. Takéto zmeny musia byť odôvodnené potrebou zabezpečiť plnú funkčnosť, spoľahlivosť a súlad diela s cieľovým stavom, pričom nesmú zásadne meniť podstatu riešenia ani prekročiť dohodnutý rozsah diela.

Verejný obstarávateľ požaduje dodanie všetkých výstupov, ak to ich charakter dovoľuje, v elektronickej a editovateľnej podobe. Počas realizácie jednotlivých aktivít sa dodávateľ zaväzuje spolupracovať s verejným obstarávateľom, najmä informovať ho o postupe prác, predpokladaných termínoch dodania jednotlivých výstupov a na požiadanie verejného obstarávateľa ozrejmiť dôvody, súvislosti a použité pracovné postupy, akými boli výstupy dosiahnuté.

Pri dodávaní výstupov sa dodávateľ zaväzuje verejnému obstarávateľovi odovzdať potrebné informácie a know-how, aby verejný obstarávateľ mohol úpravy a aktualizáciu všetkých výstupov podľa Kapitoly 2. Opis predmetu zákazky vykonávať vlastnými kapacitami, t. j. prostredníctvom interných zamestnancov. Verejný obstarávateľ požaduje zapojenie interných zamestnancov do prípravy výstupov vo vyššej miere s cieľom, aby bolo možné tieto výstupy naďalej udržiavať aktuálne internými kapacitami. Povinnosti uchádzača týkajúce sa zhotovenia diela týmto nie sú dotknuté.

Dodávateľ je povinný zaistiť pri poskytovaní služieb prevádzkovateľovi základnej služby dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na tretie strany v zmysle požiadaviek Zmluvy, príloh na ktoré sa odvoláva, Zákona o KB, Zákona o ITVS, vykonávacích predpisov k týmto zákonom a najlepších praktík (tzv. best practices) v oblasti kybernetickej bezpečnosti.

Dodávateľ je povinný vykonávať implementáciu nástrojov, pri ktorých možno očakávať alebo sa očakáva výpadok či obmedzenie služieb a funkcionality systémov verejného obstarávateľa, výlučne v servisnom okne určenom verejným obstarávateľom. Verejný obstarávateľ určí servisné okno s cieľom minimalizovať dopady na prevádzku, pričom toto servisné okno môže byť stanovené mimo bežnej pracovnej doby alebo počas dní pracovného pokoja.

Dodávateľ je povinný ku každému dodanému bezpečnostnému nástroju poskytnúť príslušnú dokumentáciu s popisom konfigurácie realizovanej v rámci implementácie, vrátane sprístupnenia používateľských príručiek alebo dokumentácie z tzv. knowledge base od výrobcov.

Dodávateľ zabezpečí implementáciu bezpečnostných nástrojov v súlade so špecifickými požiadavkami verejného obstarávateľa, pričom je povinný zohľadniť aj výsledky analýzy rizík kybernetickej bezpečnosti a ďalšie relevantné výstupy z Modulu č. 1: Riadenie kybernetickej bezpečnosti.

Dodávateľ je povinný vykonať optimalizáciu bezpečnostných nástrojov s cieľom zabezpečiť ich plynulú a stabilnú prevádzku bez výpadkov a nadmerného množstva falošne pozitívnych hlásení (false positive/false negative ratio), a to na požiadanie verejného obstarávateľa aj kedykoľvek v rámci trvania Zmluvy po ich akceptácii v rámci post-implementačnej fázy.

**ZAŠKOLENIE PERSONÁLU**

Na zabezpečenie plynulého odovzdania implementovaných bezpečnostných nástrojov do prevádzky ZZS Bratislava dodávateľ zabezpečí zaškolenie odborných zamestnancov verejného obstarávateľa z pohľadu práce s bezpečnostnými nástrojmi 1-4, ich predstavenie a oboznámenie so zavedenými nastaveniami a pravidlami, závislosťami a integráciami s inými informačnými systémami, ich úpravami a prispôsobením, používateľským prostredím v ovládacích konzolách, požiadavkami na

bezpečnú prevádzku (aktualizácie, patchovanie, troubleshooting, kontaktovanie supportu, popr. iná údržba systémov), a to:

- v rozsahu spolu minimálne 5 človekodní (1 človekodeň = 8 hodín, počítané po hodinách), rozvrhnuté podľa požiadaviek verejného obstarávateľa; do tohto rozsahu sa nezapočítava čas vynaložený na transfer know-how počas implementácie bezpečnostných nástrojov a poskytovaní služieb, ktoré sú definované v časti Implementačná fáza tejto kapitoly;
- prostredníctvom on-site experta v priestoroch verejného obstarávateľa alebo podľa požiadaviek verejného obstarávateľa;

Zaškolenie personálu je súčasťou IMPLEMENTAČNEJ FÁZY a je realizované po častiach, vo vyhradený čas a spravidla pri odovzdaní bezpečnostného nástroja do akceptačného konania, najneskôr ako súčasť príslušného míľnika podľa HARMONOGRAMU.

**AKCEPTAČNÉ KONANIE**

Každý výstup IMPLEMENTAČNEJ FÁZY je predmetom samostatného akceptačného konania. Dodávateľ je na požiadanie verejného obstarávateľa povinný poskytnúť primeranú odbornú súčinnosť pri testovaní a overení správnosti konfigurácií podľa Kapitoly č. 2 tohto dokumentu alebo Prílohy č. 2 Zmluvy Špecifikácia požiadaviek. AKCEPTAČNÉ KONANIE pozostáva z:

- potvrdenia preberacieho protokolu a overeniu naplnenia požiadaviek. Verejný obstarávateľ má na posúdenie, kontrolu, testovanie a akceptáciu výstupov 15 pracovných dní. V prípade pripomienok verejný obstarávateľ písomne informuje dodávateľa o nedostatkoch a vráti mu výstup na prepracovanie s určením primeranej lehoty na nápravu v súlade s podmienkami Zmluvy.
- V prípade nevznesenia žiadnych pripomienok zo strany verejného obstarávateľa sa následne pristúpi k podpisu akceptačného protokolu.

**4.2 POST-IMPLEMENTAČNÁ FÁZA**

Po dodaní a akceptácii jednotlivých výstupov dodávateľ zabezpečí postimplementačnú podporu, ktorá začína plynúť pre každý bezpečnostný nástroj individuálne, vždy odo dňa nasledujúceho po dni akceptácie príslušného výstupu. Služby postimplementačnej podpory skončia súčasne pre všetky bezpečnostné nástroje, a to uplynutím 17 mesiacov od účinnosti Zmluvy. Týmto nie je dotknutá dĺžka platnosti licencií podľa Kapitoly 3. Rozsah zákazky a licenčné podmienky.

Úspešný uchádzač v rámci licenčného obdobia zabezpečuje, aby došlo k naplneniu podpory (tzv. supportu) v rozsahu požiadaviek definovaných v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek počas obdobia platnosti licencie jednotlivých systémov a bezpečnostných nástrojov.

<u>Súhrn činností:</u>

a. Ladenie bezpečnostných nástrojov 1-4, znižovanie false positive/false negative ratio, optimalizácia prevádzky.
b. Poskytovanie služby proaktívneho bezpečnostného monitoringu v zmysle požiadaviek Kapitoly 2. Opis predmetu zákazky, bod 3.3 Služby bezpečnostného monitoringu.

c. Úspešný uchádzač v rámci licenčného obdobia zabezpečuje, aby došlo k naplneniu podpory (tzv. supportu) v rozsahu požiadaviek definovaných v Prílohe č. 2 Zmluvy Špecifikácia požiadaviek počas obdobia platnosti licencie jednotlivých bezpečnostných nástrojov.

Minimálne požiadavky na post-implementačnú podporu pre bezpečnostný nástroj 1:

a. Správa a údržba systému,
b. Podpora pri spracovaní a hodnotení bezpečnostných auditov a záznamov,
c. Vykonávanie pravidelnej revízie nastavení a konfigurácie systému,
d. Údržba a aktualizácie podľa legislatívnych zmien,
e. Monitoring správnosti dátovej synchronizácie a integrácií, ak sú,
f. Zabezpečenie komunikácie s výrobcom bezpečnostného nástroja.

Minimálne požiadavky na post-implementačnú podporu pre bezpečnostnému nástroju 2:

a. Monitoring dostupnosti a výkonu zariadení,
b. Správa aktualizácií firmvéru a bezpečnostných signatúr,
c. Vykonávanie pravidelného auditu bezpečnostných politík a logov,
d. Konzultácie a návrhy zmien pri zmenách v sieťovej infraštruktúre,
e. Zabezpečenie komunikácie s výrobcom,
f. Návrhy na optimalizáciu pokrytia a výkonnosti.

Minimálne požiadavky na post-implementačnú podporu pre bezpečnostný nástroj 3:

a. Overovanie pripojenia, synchronizácie a aktualizácie politiky,
b. Údržba a aktualizácia detekčných pravidiel a politiky,
c. Konzultácie pri škálovaní a úpravách architektúry nasadenia,
d. Zabezpečenie komunikácie s výrobcom,
e. Návrhy na optimalizáciu pokrytia a výkonnosti systému.

Minimálne požiadavky na post-implementačnú podporu pre bezpečnostný nástroj 4:

a. Monitoring a dostupnosť služby,
b. Konzultácie k detekčným pravidlám, custom alerts, log parsing,
c. Správa napojení na logovacie zdroje,
d. Priebežné ladenie a optimalizácia korelačných pravidiel,
e. Vykonávanie pravidelných testov funkčnosti logovacích zdrojov a alertingu,
f. Zabezpečenie komunikácie s výrobcom.

Všetky vyššie uvedené aktivity súvisiace s post-implementačnou podporou nástrojov 1-4, musia byť realizované v súlade s nižšie uvedeným časovým harmonogramom. Na zabezpečenie všetkých požadovaných aktivít sa predpokladá odborná alokácia v rozsahu 36 človekodní.

**4.3 HARMONOGRAM**

Verejný obstarávateľ požaduje priebežné odovzdávanie výstupov definovaných v Kapitole 2. Opis predmetu zákazky na akceptačné konanie, a to najneskôr v termínoch podľa míľnikov uvedených v nasledujúcom harmonograme (tzv. fakturačné míľniky):

| Míľnik | Predmet | Termín |
|---|---|---|
| Míľnik č. 1 | Modul č. 1: Riadenie kybernetickej bezpečnosti (výstupy č. 1.1, 1.2 a 1.3) | Najneskôr do 6 mesiacov od účinnosti Zmluvy |
| Míľnik č. 2 | Modul č. 2: Sieťová bezpečnosť a ochrana perimetra (výstup č. 2.1) | Najneskôr do 3 mesiacov od účinnosti Zmluvy |
| Míľnik č. 3 | Modul č. 3: Ochrana kritických systémov a bezpečnostný monitoring (výstupy č. 3.1 a 3.2) | Najneskôr do 4 mesiacov od účinnosti Zmluvy |
| Míľnik č. 4 | - Modul č. 1: Riadenie kybernetickej bezpečnosti (výstup č. 1.4),<br>- Modul č. 3: Ochrana kritických systémov a bezpečnostný monitoring (výstup č. 3.3),<br>- Služby postimplementačnej podpory pre bezpečnostné nástroje 1-4. | Najneskôr do 17 mesiacov od účinnosti Zmluvy |