**OPIS PREDMETU ZÁKAZKY**

Predmetom zákazky je: **Zabezpečenie informačnej a kybernetickej bezpečnosti** ako súčasť projektu **„Zabezpečenie I&K bezpečnosti ZZ – FNsP FDR BB“**

Súčasťou predmetu zákazky sú súvisiace služby:

* inštalácia,
* konfingurácia,
* užívateľské nastavenie (customizácia),
* funkčná skúška,
* protokolárne prevzatie a odovzdanie predmetu zmluvy,
* odovzdanie dokumentácie,
* odborné zaškolenie,

V prípade, ak sa v opise predmetu zákazky uvádzajú údaje alebo odkazy na konkrétneho výrobcu, postup, značku, obchodný názov, typ, umožňuje sa uchádzačovi predloženie ponuky s ekvivalentným výrobkom, ten však musí spĺňať minimálne požiadavky uvedené v Opise predmetu zákazky, resp. musí mať rovnaké alebo lepšie technické vlastnosti.

Všetky ponúkané výrobky, služby musia byť v súlade s príslušnými požiadavkami stanovenými v právnych predpisoch EÚ.

**Použité skratky:**

I&K – Informačná a kybernetická

ZZ – zdravotnícke zariadenie

EPS – End Point Security – Koncový bod zabezpečenia

Eps – Events per second – Počet udalostí za sekundu

IKT – Informačné a Komunikačné technológie

LMS – Log Management System – Systém na menežovanie log súborov

MD – ManDay - Človekodeň

PKI – Public Key Infrastructure – Infraštruktúra poskytujúca digitálny certifikát, slúžiaci pre neskoršiu identifikáciu osôb

SIEM – Security Incident and Event Management – Monitorovanie a analýza log. záznamov generovanými IS

SOC – Security Operation Center – real-time znalosť bezpečnostnej situácie v infraštruktúre

Predmet zákazky je rozdelený na aktivity s požadovanými profesiami resp. technickými prostriedkami uvedenými v prílohe – Cenová ponuka k zmluve o zabezpečení informačnej a kybernetickej bezpečnosti:

* Aktivita 1: Analýza a dizajn
* Aktivita 2: Implementácia a testovanie
* Aktivita 3: Nasadenie
* Aktivita 4: Cena licencií súvisiacich s prevádzkou HW/SW (od 01.11.2023 – 31.10.2024)

Cena bude ocenená na základe požiadaviek na riešenie – opis predmetu zákazky uvedený nižšie. Túto aktivitu oceňte pre každú časť riešenia v priloženom súbore: Príloha - Cenová ponuka k zmluve o zabezpečení informačnej a kybernetickej bezpečnosti.

V požiadavkách na riešenie – opis predmetu zákazky je vyšpecifikované, pri častiach riešenia. Verejný obstarávateľ predpokladá dodanie licencií.

V prípade, že Vami oceňované riešenie predpokladá dodanie aj iných licencií, je potrebné tieto licencie v predmetnej tabuľke vyšpecifikovať a súčasne uviesť počet kusov.

**Zabezpečenie informačnej a kybernetickej bezpečnosti (do 31.10.2023)**

1. Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM)
2. Modul SIEM – tvorený službou poskytovanou špecialistami a SW licenciami technológie SIEM pre 800EPS
3. Modul SOC - implementáciu SOC služby v režime min. 8 hodín/ počas 5 pracovných dní, nasadenie SOC služby, vyškolenie obsluhy, prevádzka služby SOC – do 31.10.2023 v rámci pilotnej prevádzky

Táto položka je financovaná z Európskych štrukturálnych a investičných fondov Operačného programu II

Prehľadná tabuľka pre položku č.1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Č.p. | Názov položky | Druh položky | Projektový manažér IT  Projektu - počet MD | IT analytik počet MD | Špecialista pre bezpečnosť IT počet MD | IT/IS konzultant počet MD | celkom MD |
| 1 | Riadenie kontinuity (BCM) | služba | 2 | 28 | 7 | 37 | 74 |
| 2 | Modul SIEM | služba | 3 | 34 | 9 | 46 | 92 |
| 3 | Licencie SIEM | tovar | --- | --- | --- | --- | --- |
| 4 | Modul SOC | služba | 2 | 20 | 5 | 26 | 53 |
| Celkom | | | 7 | 82 | 21 | 109 | **219** |

Tabuľka sadzieb určených MIRRI (Ministerstvo investícií, regionálneho rozvoja a informatizácie) a podľa ŽoNFP (Žiadosť o nenávratný finančný príspevok)

|  |  |  |  |
| --- | --- | --- | --- |
| Pracovné pozície | Maximálna sadzba špecialistu bez DPH (určená MIRRI) | Sadzba špecialistu bez DPH (určená ŽoNFP) | Spolu počet MD určený  ŽoNFP |
| Projektový manažér IT projektu | 890 € | 500 € | 7 |
| IT analytik | 740 € | 450 € | 82 |
| Špecialista pre bezpečnosť IT | 1 200 € | 619 € | 21 |
| IT/IS konzultant | 900 € | 448 € | 109 |
| **Celkom** | | | **219** |

1. **Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17).**

Kontinuita činností musí zadefinovať scenáre rôznych udalostí, ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

* náhla nedostupnosť personálu či nepoužiteľnosť pracoviska/budovy,
* nedostupnosť technologickej infraštruktúry či potrebných médií,
* incident či živelná katastrofa.

V rámci kontinuity činností musia byť stanovené požiadavky na zdroje (adekvátne finančné, materiálno-technické a personálne zdroje), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti sa musí určiť čo má byť:

* hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch,
* strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalším stratám.

Súčasťou kontinuity činností musí byť vypracovanie analýzy funkčných dopadov a kvalifikácia potencionálnych dopadov a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu musí byť určenie:

* cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
* cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby.

Kontinuitou musia byť zavedené postupy zálohovania na obnovy siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:

1. frekvenciu a rozsah zdokumentovania a schvaľovania obnovy záloh,
2. určenie osoby zodpovednej za zálohovanie,
3. časový interval, identifikáciu rozsahu údajov, zadefinovanie dátového média zálohovania a zabezpečenie vedenia dokumentácie o zálohovaní,
4. umiestnenie záloh v zabezpečenom prostredí s riadeným prístupom,
5. zabezpečenie šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
6. vykonávanie pravidelného preverenia záloh na základe vypracovaného plánu, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

Kontinuita činností musí obsahovať minimálne:

* plán kontinuity na stanovenie požiadaviek a zdrojov,
* plán reakcie na incidenty a plány havarijnej obnovy prevádzky,
* politiku a ciele kontinuity, analýzu funkčných dopadov,
* stratégiu riadenia kontinuity vrátane evakuačných postupov,
* plán údržby a kontroly BCMS.

Pre koordináciu vstupov a implementáciu výstupov do a so služby SOC musí byť kontinuita činností zabezpečená nasadením IS pre vyhodnotenie a riadenie hrozieb, aktív, zraniteľností a s tým súvisiacich opatrení. Tento IS musí byť typu klient – server nasadený u obstarávateľa na jeho serveri bez závislosti na cloudových službách, aktualizáciách cez internet a inom komerčnom programovom vybavení okrem operačného systému.   
  
Informačný systém pre vyhodnotenie a riadenie hrozieb, aktív, zraniteľností a s tým súvisiacich opatrení musí spĺňať tieto funkčné vlastnosti:

* správa aktív a zraniteľností – vedenie zoznamu aktív a zraniteľností, vrátane ich vlastníkov,
* správa hrozieb a opatrení – vedenie zoznamu rozpoznaných hrozieb a opatrení,
* správa vzťahov – evidencia rozpoznaných vzťahov medzi aktívami a zraniteľnosťami,
* správa rizík semikvantitatívnou prípadne kvantitatívnou metódou hodnotenia významnosti rizík vyjadrená číselne a následne kategorizovaná.

**Verejný obstarávateľ požaduje dodať a implementovať** v rámci poskytovanej služby vypracovania kontinuity aj informačný systém pre vyhodnotenie a riadenie hrozieb, aktív, zraniteľností a s tým súvisiacich opatrení s časovo neobmedzenou licenciou IS pre dvoch používateľov, ako aj zrealizovať inštaláciu na serveroch verejného obstarávateľa. **Verejný obstarávateľ požaduje oceniť, vytvoriť a zaviesť kontinuitu činností v plnom rozsahu stanovenom zákonom č.: 69/2019 Z. z. o kybernetickej bezpečnosti a vyhláškou č.: 362/2018 Z. z. vrátane IS pre vyhodnotenie a riadenie hrozieb, aktív, zraniteľností a s tým súvisiacich opatrení,** ako aj implementovať procesy kontinuity a IS v podmienkach verejného obstarávateľa, vyškoliť zamestnancov verejného obstarávateľa a zabezpečiť výkon špecialistu (manažéra pre riadenie kontinuity) až do termínu 31.10.2023.

**B) Modul SIEM**

Funkčné požiadavky:

* riešenie bude postavená na analýze súčasnej IT infraštruktúry a prevádzky základnej služby s cieľom identifikovať zdroje údajov pre SIEM, úroveň a spôsob zaznamenávania a zberu denníkov udalostí ako aj ich rozsah a komplexnosť obsiahnutých informácií
* následne bude vypracovaný návrh optimalizácie systému zberu a uchovávania denníkov udalostí (návrh LMS), ktorý bude po odsúhlasení implementovaný
* návrh optimalizácie systému zberu a uchovávania denníkov udalostí bude obsahovať zmeny s cieľom zvýšiť úroveň výpovednej hodnoty informácií zaznamenaných v denníkoch udalostí (napríklad implementáciou Sysmon z balíka Windows Sysinternals alebo podobným SW vybavením) ako aj návrh retenčných politík vychádzajúcich zo zoznamu spracovateľských operácií nad osobnými údajmi Prevádzkovateľa a požiadaviek platnej legislatívy
* na základe vyššie uvedených záverov bude vybrané a do testovacej prevádzky zavedené softvérové vybavenie SIEM,
* Identifikácia a popis assetov (zdrojov logov), ktoré vstupujú do perimetra bezpečnostného dohľadu
* Nastavenie filtrácie a agregácie logov, ich následnú normalizáciu z rôznych zdrojov a formátov
* Nastavenie a otestovanie zberu logov a ich následné uskladnenie v online režime a otestovanie archivácie logov z online do offline režimu
* Implementácia a testovanie SIEM riešenia
* Vytváranie Use Case pre koreláciu udalostí s cieľom identifikácie incidentov
* Návrh procesnej matice na postup odstránenia incidentu
  + Spracovanie logov a iných zdrojov dát pre bezpečnostný monitoring v počiatočnom objeme približne 800 EPS, čo predstavuje cca 50-80 GB denne zo systémov verejného obstarávateľa
  + SIEM musí umožňovať prístup aj pre administrátorov verejného obstarávateľa a umožniť im plnohodnotne prehľadávať uložené logy aj bez súčinnosti dodávateľa s možnosťou uloženia rôznych „pohľadov“ na tieto logy, možnosť exportu logov a to po celú dobu retencie dát, minimálne 100 dní
  + SIEM musí umožňovať prehľady o všetkých pripojeniach a využití Internetovej linky z logov firewallu - kto, kde (IP adresa), kedy a koľko (prenesené dáta v oboch smeroch) po celú dobu retencie dát. Prehľad by malo byť možné vytvoriť tak ako pre jedného užívateľa (IP adresu) tak aj pre všetkých užívateľov za ľubovoľné obdobie.
  + SIEM musí umožňovať vykonanie analýzy a zadefinovanie návrhu spôsobu zaznamenávania logov a auditných udalostí, ich centrálneho zberu a zhromažďovania, ukladania, uchovávania, rotácie, prípadne poskytovania analýz a reportovania
  + SIEM musí umožniť vykonanie konsolidácie logov pre efektívne a spoľahlivé fungovanie SIEM
  + SIEM musí umožniť parsovanie logov – pre definované OS, sieťové zariadenia, aplikácie a pod.
  + V SIEM nástroji možnosť spracovať logy zo všetkých informačných systémov verejného obstarávateľa, ktoré budú zadefinované, čo do typu aj objemu dát
* Riešenie musí mať centrálnym dashboard – webovú aplikáciu s centrálnym riadiacim panelom pre jednotný pohľad na aplikácie a systémy prevádzkovaných v security operation centre
  + Súčasťou prevádzkovania nástroja bude jeho pravidelná údržba min. v rozsahu:
  + kontrola dát,
  + asset manažment, access manažment,
  + aktualizácie,
  + ostatné činnosti prevádzkového charakteru.
  + Možnosť rozšírenia bezpečnostného monitoringu pre nové informačné technológie žiadateľa minimálne do odhadnutého počtu nových zariadení, ktoré pribudnú verejnému obstarávateľovi do konca doby podpory (min. 5 rokov)
  + Prevádzkovanie SIEM nástroja musí umožniť verejnému obstarávateľovi výkon kontrolnej činnosti alebo auditu v súlade s Vyhl. NBÚ č.362/2018, § 8, ods. 2, písm. h)
  + Pri riešení technológie musí Dodávateľ zvlášť oceniť službu poskytovanú svojimi špecialistami a SW licencie technológie SIEM pre 800EPS s platnosťou 1 rok. (od 01.11.2023)

Ďalšie požiadavky na technológiu SIEM:

* SIEM nesmie byť obmedzovaný počtom zdrojov udalostí (logov).
* SIEM nesmie byť licenčne obmedzený počtom používaných korelačných pravidiel, pretože nemožno vopred určiť finálny počet týchto pravidiel.
* SIEM musí poskytovať centrálnu webovú konzolu, z ktorej je možné spravovať celé riešenie.
* SIEM musí podporovať integráciu pomocou otvoreného API rozhrania. API môže slúžiť pre strojovú interakciu s riešením alebo pre integráciu s riešeniami tretích strán.
* SIEM musí podporovať prácu s reputačnými službami výrobcu alebo s reputačnými službami tretích strán. Reputačné služby poskytujú napríklad IP geolokáciu, botnet kanály atp. Súčasťou riešenia bude licencia pre využitie reputačné služby výrobcu.
* Riešenie musí byť dodané v preferovanej forme objednávateľa v možnej kombinácii Virtual alebo HW a Virtual alebo Cloud.
* Riešenie musí byť dodané formou distribuovanej architektúry, kedy komponent pre spracovanie a ukladanie udalostí na úložisko bude vo forme HW zariadenia a všetky ostatné komponenty môžu byť umiestnené vo forme virtuálneho zariadenia do virtuálneho prostredia.
* Umelá inteligencia musí v rámci ponúkaného riešenia sledovať históriu riešenie útokov bezpečnostnými analytikmi a na jej základe odporúčať ďalšie kroky.
* Riešenie musí licenčne a výkonovo podporovať rozšírenie počtu spracovania EPS bez nutnosti dokúpenia/navyšovania licencií pri rovnakej infraštruktúre objednávateľa.
* Riešenie musí licenčne a výkonovo podporovať rozšírenie počtu spracovania Flow (Záznam toku dát) bez nutnosti dokúpenia/navyšovania licencií pri rovnakej infraštruktúre objednávateľa.
* Riešenie musí mať schopnosť uchovať interne (tzv. Online) aspoň 70 TB dát bez toho, aby riešenie vyžadovalo použitie externých pamäťových zariadení alebo médií.
* Podpora a údržba pre HW zariadenie a softvér musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) a musí byť realizovaná onsite v režime 24x7 s reakčnou dobou pri kritických problémoch 2 hodiny (best effort).
* Riešenie musí licenčne podporovať analýzu sieťových údajov v reálnom čase, aby bolo možné odhaľovať stopy a skryté bezpečnostné hrozby v mnohých scenároch predtým, ako môžu poškodiť organizáciu, vrátane phishingových e-mailov, malvéru, exfiltrácie údajov, zneužívania DNS a iných aplikácií atď.
* Riešenie musí licenčne podporovať nepretržitý monitoring zaznamenaných „flows“ v sieti, aby bolo možné identifikovať anomálnu prevádzku. Riešenie musí poskytovať vizualizácie podozrivých záznamov, ktoré sa najviac líšia od ostatných záznamov pozorovaných v rámci siete. Musí taktiež podporovať rýchlu identifikáciu flow-ov s podozrivým správaním v sieti a uprednostniť ich vyšetrovanie.

**C) Modul SOC**

Opis procesov a funkčné požiadavky k uvedeniu služby SOC:

* Primárnym cieľom aktivity je prenesenie zodpovednosti za výkon služby Security Operation Center na dodávateľa formou služby.
* Analýza prostredia pre vytvorenie architektúry nasadenia nevyhnutných HW prostriedkov u odberateľa
* Implementácia HW (kolektor, sonda) u verejného obstarávateľa
* Vypracovanie, odsúhlasenie zabezpečeného prepojenia prostredia verejného obstarávateľa a poskytovateľa služieb SOC (dáta musia byť prenášané v zašifrovanej forme a musia byť chránené voči neoprávneným zmenám a zásahom (zachovanie integrity dát)
* Testovanie funkčnosti HW prostriedkov a prepojenia prostredia verejného obstarávateľa a poskytovateľa služieb SOC
* Implementácia, testovanie a uvedenie do pilotnej prevádzky Security Ticketingu
* Implementácia, testovanie a uvedenie do pilotnej prevádzky jednotného Security Dasboardu a SOAR
* Procesné, technické nastavenie a otestovanie riešenia na detailné auditovanie aktivity špecialistov SOC. Daný nástroj na zaistenie auditnej stopy je súčasťou technického riešenia dodávateľa.
* Procesné, technické nastavenie a otestovanie riešenia na real-time prevádzkový monitoring bezpečnostných technológií nasadených v službe SOC
* Vypracovanie a otestovanie procesnej a komunikačnej matice pre špecialistov bezpečnostného monitoringu u dodávateľa služby SOC a incident response tímu na strane verejného obstarávateľa
* Tvorba a pravidelné ladenie RUNBOOKS pre efektívne riadenie bezpečnostných udalostí
* Tvorba a udržiavanie Knowledge Base (na základe vzniknutých udalostí) MITRE ATT&CK.
* Nastavenie tvorby databázy všetkých identifikovaných aktivít (autodiscovery)
* Vypracovanie dokumentácie (logovacieho štandardu)
* Poskytnutie pravidelného mesačného reportingu
* Integrácia riešenia služieb SOC s Threats Exchange na úrovni MISP
* Pravidelné školenie u verejného obstarávateľa pre oblasť kybernetickej bezpečnosti
* Produkčná prevádzka bude nasledovať po preverení funkčnosti služby prostredníctvom simulovaných incidentov.
* Aktivita Zriadenie SOC ako služby je rozdelená do nasledovných krokov:
  + - Vstupná analýza IT infraštruktúry a prevádzky základnej služby pre potreby procesného nastavenia služby SOC
    - Návrh komunikačných pravidiel, matice zodpovedností a procesov služby SOC
    - Realizácia výberového konania
    - Spustenie služby v testovacej prevádzke
    - Testovanie komunikačných pravidiel, matice zodpovedností a procesov služby SOC
    - Implementácia služby SOC do produkčnej prevádzky
    - Zaškolenie personálu verejného obstarávateľa
* Verejný obstarávateľ požaduje oceniť aktivitu zriadenie SOC služby nasledovne:
  + Analýzu a implementáciu SOC služby v režime min. 8 hodín/ počas 5 pracovných dní
  + Nasadenie SOC služby
  + Vyškolenie obsluhy
  + Prevádzka služby SOC – do 31.10.2023 v rámci pilotnej prevádzky

Zoznam zariadení a IS Verejného obstarávateľa:

|  |  |  |
| --- | --- | --- |
| **Fakultná nemocnica s poliklinikou F.D. Roosevelta Banská Bystrica** | **Aktuálny počet zariadení** | **Predpokladaný počet zariadení po 5 rokoch** |
| Windows Servery | 39 | 50 |
| Windows AD DC servery | 2 | 2 |
| Linux / Unix servery | 35 | 45 |
| Virtualizácia (počet nodov, typ virtualizácia) | 80 | 100 |
| Diskové polia | 5 | 5 |
| Windows Desktopy / Notebooky | 1200 | 1300 |
| **Síeťová infraštruktúra** | | |
| Sieťové routre, FW | 4 | 4 |
| Sieťové CORE switche | 4 | 4 |
| Sieťové WiFi - Controler | 1 | 2 |
| Sieťové WiFi - AP | 25 | 90 |
| Celkový počet Aktívnych prvkov (manažovateľných) | 110 | 130 |
| **Bezpečnostná infraštruktúra** | | |
| VLAN | 57 | 65 |
| VPN brány | 2 | 2 |
| Antivírusoví klienti – ESET Antivírus | 1150 | 1350 |
| **Aplikácie** | | |
| Celkový počet Aplikácií 30 z toho významných 5 ( NIS – Nemocničná Informačný Systém + moduly; PACS – Obrazový Archivačný Systém; Lekáreň; ERP; PAM) | Celkový počet Aplikácií 30 z toho významných 5 | Celkový počet Aplikácií 35 z toho významných 10 |
| Web Servery (IIS, Apache, Tomcat) | 15 | 25 |
| Databázy (MSSQL, Oracle, PostgreSQL, MySQL) - počet inštancií | 17 | 20 |
| Email - (počet užívateľov) | 1020 | 1200 |

Návrh riešenia uchádzača:

*(Uchádzač navrhne riešenie, ktoré bude zohľadňovať min. všetky požiadavky z opisu predmetu zákazky a zároveň uvedie bližší popis požiadaviek pre „Zabezpečenie informačnej a kybernetickej bezpečnosti“).*

Obchodné meno uchádzača: .............................................................. *(doplní uchádzač)*

Sídlo alebo miesto podnikania uchádzača: ........................................ *(doplní uchádzač)*

IČO uchádzača: ..................................................................................*(doplní uchádzač)*

V.........................................., dňa ..........................

...........................................................................

meno a priezvisko štatutárneho zástupcu

podpis a pečiatka uchádzača