**OPIS PREDMETU ZÁKAZKY**

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

Súčasťou predmetu zákazky sú súvisiace služby:

* konfingurácia,
* užívateľské nastavenie (customizácia),
* zabezpečenie prevádzky počas 60 mesiacov (od 01.11.2023),

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:

* Aktivita 1: Cena služieb súvisiaca s prevádzkou navrhovaného riešenia

Cena bude ocenená na základe požiadaviek na riešenie – opis predmetu zákazky uvedený nižšie. Túto aktivitu oceňte podľa prílohy, v priloženom súbore: Príloha – Cenová ponuka k zmluve o zabezpečení prevádzky služieb informačnej a kybernetickej bezpečnosti.

* Aktivita 2: Cena za dodanie potrebného HW/SW

Cena bude ocenená na základe požiadaviek na riešenie – opis predmetu zákazky uvedený nižšie. Túto aktivitu oceňte pre každú časť riešenia v jednotlivých hárkoch dokumentu, priloženom súbore: Príloha - Cenová ponuka

Verejný obstarávateľ nepredpokladá dodanie HW pre navrhované riešenie. V prípade, že Vami oceňované riešenie predpokladá dodanie HW, je potrebné tento HW v predmetnej tabuľke vyšpecifikovať a súčasne uviesť počet kusov.

* Aktivita 3: Cena licencií súvisiacich s prevádzkou HW/SW

Cena bude ocenená na základe požiadaviek na riešenie – opis predmetu zákazky uvedený nižšie. Túto aktivitu oceňte pre každú časť riešenia v Prílohe - Cenová ponuka k zmluve o zabezpečení prevádzky služieb 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 prevádzky počas 60 mesiacov od 01.11.2023 do 31.10.2028**

Táto položka je financovaná z vlastných prostriedkov verejného obstarávateľa

**Zabezpečenie prevádzky počas 60 mesiacov po ukončení implementácie a nasadenia BCM, SIEM a SOC od 01.11.2023**

Požiadavky na zabezpečenie bezpečnostného monitoringu informačných systémov verejného obstarávateľa tak, aby bola zaistená dôvernosť, dostupnosť a integrita dátových aktív a základných služieb v súlade so zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti počas 60 mesiacov od 01.11.2023.

Služby bezpečnostného monitoringu musia byť poskytované prostredníctvom SOC (Security Operation Centra), ktorého súčasťou je CSIRTu (Computer Security Incident Response Team) takým spôsobom, aby bola zaistená prvotná reakcia na vzniknutý incident s prvotnou analýzou príčin vzniku bezpečnostnej udalosti a jej popisom a odovzdanie udalosti na riešenie obstarávateľovi.

Dodávateľ služby SOC a CSIRT musí súčasne disponovať kapacitami na následné vypracovanie návrhov opatrení na elimináciu dopadu bezpečnostnej udalosti na informačné systémy obstarávateľa.

Zároveň dodávateľ musí zabezpečiť kontinuitu podpory (maintenance) licencií 800EPS dodávaných ako súčasť riešenia SIEM na obdobie 48 mesiacov.

**Špecifikácia služieb zabezpečenia prevádzky**:

1. Poskytovanie služby bezpečnostného monitoringu (za pomoci technológií) v režime 24 X 7 so zabezpečením automatickej notifikácie udalostí
2. Poskytovanie služby bezpečnostného monitoringu na úrovni L1 (Operátor) v režime 8 x 5 v rozsahu §14, ods. 4 a §15, ods. 2 Vyhl. NBÚ č.362/2018
3. Poskytovanie služby na úrovni L2 a L3 (analytik, špecialista LM a SIEM, procesy SOC-u)
4. Tvorba USE CASE podľa procesov, technológií a potrieb Verejného obstarávateľa
5. Konfigurácia SIEM podľa incidentov min. 1 x za 3 mesiace (zahrnúť do služby SOC)
6. Licenčné pokrytie LM a SIEM technológie – 800 EPS počas 48 mesiacov
7. Online a offline ukladanie logov (retencia 180 dní, archivácia 13 mesiacov)
8. Pre potreby ukladania logov je povinný dodávateľ zabezpečiť v rámci poskytovanej služby aj diskové úložisko s min. kapacitou 20TB prevádzkované v sídle verejného obstarávateľa s pripojením na servery verejného obstarávateľa (pripojenie min. 1Gbps)
9. Službu manažéra pre riadenie kontinuity od 31.10.2023 zabezpečí Verejný obstarávateľ vlastnými kapacitami.

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 požadovaných „Špecifikácií služieb zabezpečenia prevádzky“).*

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