**Příloha č. 1 – Specifikace předmětu plnění**

**Název zakázky:** Zajištění služby kybernetického bezpečnostního dohledu
**Číslo zakázky:** P22V00000003
**Zadavatel:** Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

## 1. Cena služby

| | ks | Celková cena bez DPH | DPH | Celková cena včetně DPH |
|---|---|---|---|---|
| **A. Měsíční paušální cena za poskytování služby kybernetického bezpečnostního dohledu** | 36 měsíců | **1.076.364,00 Kč** | **21%** | **1.302.400,44 Kč** |
| **B. Cena za konzultaci** | 36 hod. | **39.204,00 Kč** | **21%** | **47.436,84 Kč** |
| **C. Cena za zahájení řešení kybernetického bezpečnostního incidentu technickým specialistou nejpozději do 2 hod.** | 36 hod. | **53.604,00 Kč** | **21%** | **64.860,84 Kč** |
| **CELKEM** | | **1.169.172,00 Kč** | **21%** | **1.414.698,12 Kč** |

## 2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem plnění veřejné zakázky je poskytnutí služby kybernetického bezpečnostního dohledu zajišťující bezpečnost IT provozu pomocí bezpečnostního týmu uchazeče. Veřejná zakázka dále zahrnuje předprojektovou analýzu, pronájem SIEM ve formě hardwarové appliance na které běží potřebný SW, instalace a konfigurace jak hardwarových tak i softwarových částí nezbytných pro poskytování služby, zaškolení zaměstnanců IT objednatele, dodání dokumentů (návodů a nastavení konfigurace), testovací provoz a zahájení poskytování služby.

### 2.1 Popis stávajícího prostředí

Stávající infrastruktura magistrátu města Frýdku-Místku obsahuje dva produkční servery a jeden testovací server, na kterých je provozována virtualizace VMware vSphere 6.7. Virtualizační platforma je centrálně spravována přes vCenter 6.7. Dále je součásti IT infrastruktury centrální diskové pole SAN a uložiště NAS. Síťová infrastruktura na všech budovách propojených optickými trasami zahrnuje přístupové a core switche HPE a dále WiFi přístupové body Aruba. Zadavatel si vyhrazuje právo na změnu infrastruktury v průběhu plnění veřejné zakázky a uchazeč na změny musí neprodleně do 14 dnů reagovat úpravami konfigurace HW a SW komponent kybernetického bezpečnostního dohledu.

### 2.2 Technické parametry

Uchazeč musí dodat plně funkční a úplně nakonfigurovaný systém dle svých nejlepších znalostí a svědomí, splňující veškeré níže uvedené minimální technické parametry a funkce tak, aby mohl poskytovat službu kybernetického bezpečnostního dohledu.

- Integrovaný systém zpracovávání logů, flow a událostí ze zadavatelem definovaných zdrojů
- Pronájem SIEM formou HW appliance
- Implementace HW a SW částí
- Měsíční profylaxe HW a SW částí

- Komunikace týmu uchazeče se zadavatelem v českém jazyce
- Pravidelná aktualizace software
- Sběr a ukládání logů, flow a událostí ze zdrojů zadavatele pro potřeby vyhodnocování bezpečnostním týmem uchazeče a jejich uložení pro případy eventuálního vyšetřování nebo provádění analýz (zdrojem se rozumí HW i SW s IP adresou včetně OS)
- Nastavení sběru logů pro konkrétní zdroje
- Zpracování logů generovaných i samotným zařízením SIEM
- Zpracování informací z flowmon sondy zachytávající síťovou komunikaci na aktivních prvcích
- Prohledávání a filtrování logů
- Předdefinované i uživatelsky definovatelné profily pro detekce kybernetických bezpečnostních událostí
- Provádění korelace, analýzy a vyhodnocení logů, flow a událostí ze zdrojů zadavatele v reálném čase
- Uživatelsky přívětivé grafické uživatelské prostředí GUI dostupné přes webové rozhraní s využitím protokolu https
- Grafické znázornění významných událostí – grafy, četnosti, časová osa atd.
- Vytvoření a přizpůsobení dashboardu pro zobrazení událostí dle požadavků zadavatele Umožnění přístupu do SIEM systému zadavateli s minimálními oprávněními pro čtení ve všech částech systému
- Zobrazení SIEM systémem zachycených a vyhodnocených potenciálních bezpečnostních událostí na náhledové obrazovce v kancelářích zaměstnanců odboru IT
- Zajištění monitorování zdrojů ve smyslu kontroly dostupnosti
- Podpora pro vzdálené i ruční instalace agentů
- Instalace agentů uchazečem
- Zabezpečená replikace všech kybernetických bezpečnostních událostí, alertů a incidentů na federační servery uchazeče, které jsou umístěny v jeho prostředí
- Analýza kybernetických bezpečnostních událostí a identifikace možných kybernetických bezpečnostních incidentů
- Identifikace kybernetických bezpečnostních incidentů včetně proaktivní komunikace o způsobu jejich řešení
- Správa uživatelů s možností intergace s MS Active Direcotry včetně podpory lokálních uživatelů
- Podporované protokoly minimálně: snmp, ftp, sftp, netflow, nfs, cifs, wmi
- Zpracovávání 1500 EPS (events per second)
- Vytvoření kompetenční a komunikační matice
- Vykonávání kybernetického bezpečnostního dohledu 24x7, zahájení řešení bezpečnostního incidentu, možnost kontaktu uchazeče zadavatelem s žádostí o řešení problému spojeného s poskytovanou službou, s žádostí o konzultaci
- Možnost zasílání SMS zpráv nebo emailů na vybraná tel. čísla nebo adresy na základě vydefinovaných událostí různých zdrojů zadavatele (např. výpadek el. napájení a přechodu UPS na baterie, výpadek switche, atd.)
- Zajištění záruky v podobě výměny vadné části případně celé HW appliance s odpovídajícími parametry. Maximální doba výpadku poskytované služby kybernetického bezpečnostního dohledu 48 hodin od nahlášení nebo detekce závady.
- Jednotné kontaktní místo pro příjem požadavků, hlášení o kybernetických bezpečnostních incidentech, pro proaktivní komunikaci a pro komunikaci i s třetí stranou (např. NUKIB, NBU, ÚOOÚ atd.)

- Informování o potvrzeném bezpečnostním incidentu analytikem uchazeče bezprostředně a neodkladně po jeho zjištění dohodnutou cestou (podpora min. pro email, sms, telefonní hovor na tel. číslo dohodnuté v komunikační matici)
- V případě detekce kybernetického bezpečnostního incidentu uchazeč musí garantovat zahájení řešení technickým specialistou nejpozději do 2 hod.
- Uchazeč musí poskytnout informaci o detekci kybernetického bezpečnostního incidentu a proaktivní komunikaci o možných řešeních se zadavatelem i třetí stranou (např. NUKIB, NBU, ÚOOÚ atd.)
- Nabízené řešení musí být v souladu s požadavky vyhlášky 316/2014 Sb., jakožto prováděcím pokynem zákona č. 181/2014 Sb. (ZoKB).
- Uchazeč musí zadavatele informovat o známých a objevených hrozbách na provozovaných systémech uchazeče bezprostředně po jejich odhalení
- Vlastní řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů je nad rámec měsíční paušální platby a řídí se cenou uvedenou v bodě 1. Cena dodávky
- Uchazeč musí zasílat 1x měsíčně souhrnný měsíční report, který bude obsahovat minimálně informace o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech, top 10 seznam koncových stanic s největším síťovým provozem, top 10 seznam s nejvíce pokusy o napadení včetně návrhů opatření. Dále report o nejfrekventovanějších komunikacích a report o zranitelnostech (vulnerability report).

## 2.3 Výčet zdrojů zadavatele

| **Zdroje** | **Výrobce** | **Kusy** |
|---|---|---|
| HW + VM Linux servery | | 11 |
| HW + VM Windows servery | | 31 |
| VM appliance (libovolný OS) | | 10 |
| Virtualizační nody | 2x Huawei, 1x HPE, 1x Lenovo | 4 |
| HW Firewall | Fortinet | 2 |
| Switches | HPE | 37 (10 IRF stacků) |
| WiFi AP | Aruba (jedno AP je v režimu kontroler) | 18 |
| SAN + NAS | Huawei, Synology | 2 |
| LAN tiskárny (výběr pro dohled) | Konica Minolta, Canon, Develop | 10 |
| Možnost rozšíření o další zdroje | | cca 10/rok |

## 2.4 Požadavky na implementaci

- Součástí poskytování služby kybernetického bezpečnostního dohledu bude instalace a implementace veškerých potřebných součástí v místě plnění
- instalace a konfigurace veškerých SW části
- napojení a konfigurace zdrojů zadavatele na nabízený systém
- instalace agentů na zdroje zadavatele
- vypracování a dodání podrobné technické dokumentace podle skutečného nasazení pro zaměstnance odboru IT zadavatele v elektronické podobě (ve formátu MS Office 2013 a vyšší), která musí obsahovat minimálně technický popis řešení, potřebné komunikační porty, kompletní popis konfigurace + nastavení a komunikační a kompetenční matici.

Technická dokumentace se po předání zadavateli stává jeho majetkem a může s ní nakládat dle svých potřeb).

Bezodstávkové instalace a konfigurace můžou probíhat za provozu. Práce, které vyžadují odstávku je možno provádět po pracovní době po předešlé domluvě.

Odstávky je možno provádět po domluvě v těchto časech:

- pondělí a středa od 17:00 do 19:00
- úterý a pátek od 14:00 do 19:00
- čtvrtek od 15:00 do 19:00
- odstávky po 19 hod. a o víkendu je možno realizovat po individuální domluvě

## 2.5 Harmonogram

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění, jenž začíná v čase T a v němž jsou uvedeny maximální možné lhůty pro jednotlivé významné milníky této veřejné zakázky.

Uchazeč připraví podrobný harmonogram prací před započetím realizace veřejné zakázky v čase T, který musí schválit obě strany.

| | |
|---|---|
| Zahájení implementace | T + 0 dní |
| Předprojektová analýzy prostředí zadavatele a příprava v místě plnění za přítomnosti zaměstnance zadavatele z odboru IT | T + 7 dní (7 dní) |
| Dodávka nabízeného HW a SW | T + 40 dní (47 dní) |
| Konfigurace nabízeného HW a SW včetně napojení zdrojů zadavatele | T + 14 (61 dní) |
| Zkušební provoz | T + 7 dní (68 dní) |
| Školení zaměstnanců zadavatele, tvorba dokumentace | T + 5 dní (73 dní) |
| Předání díla | T + 1 den (74 dní) |

## 2.6 Školení zaměstnanců zadavatele

Uchazeč zajistí školení zaměstnanců zadavatele z odboru IT na veškeré součásti nabízeného systému

- školení musí probíhat v místě plnění VZ a v rozsahu potřebném pro využívání služby nabízeného systému (ukázka, popis, nastavení a vysvětlení jednotlivých součástí systému) minimálně v rozsahu 8 hodin
- školení musí rovněž zahrnovat ukázky alertů a reportů včetně popisu a vysvětlení
- školení se zúčastní 2-3 administrátoři (k dispozici je školící místnost s prezentační technikou v místě plnění)
- náklady na školení musí být zahrnuty v nabídkové ceně k položkám, ke kterým se vztahují