Příloha č. 1 – Specifikace předmětu plnění

Název zakázky: Zajištění služby kybernetického bezpečnostního dohledu
Číslo zakázky: P23V00000096

1. Cena služby

	ks	Celková cena bez DPH	DPH	Celková cena včetně DPH
A. Měsíční paušální cena za poskytování služby kybernetického bezpečnostního dohledu	48 měsíců	**2.654.400,-Kč**	**21 %**	**3.211.824,-Kč**
B. Cena za práce nad rámec měsíčního paušálu (např. řešení kybernetických bezpečnostních hrozeb a incidentů, konzultací atd.)	48 hod.	**86.400,-Kč**	**21 %**	**104.544,-Kč**
CELKEM		**2.740.800,-Kč**	**21 %**	**3.316.368,-Kč**

2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem zakázky je komplexní zajištění služby kybernetického bezpečnostního dohledu typu Security Operations Center (dál jen služby SOC) na dobu 48 měsíců zajišťující bezpečnost IT provozu pomocí bezpečnostního týmu poskytovatele. Služby SOC budou zajišťovány formou pronájmu nástrojů typu SIEM pro vyhodnocování kybernetických bezpečnostních událostí v komunikačních sítích magistrátu. Dále formou pronájmu bude zajištěna služba hlídání a blokace nelegitimních DNS dotazů. Zakázka dále zahrnuje předprojektovou analýzu, instalaci a konfiguraci hardwarových i softwarových částí nezbytných pro poskytování služby, zaškolení zaměstnanců IT objednatele, testovací provoz, nastavení komunikace mezi objednatelem a poskytovatelem, vydefinování rozsahu reportů a zahájení poskytování služby.

2.1 Popis stávajícího prostředí

Stávající infrastruktura magistrátu města Frýdku-Místku obsahuje dva produkční servery a dva testovací servery, na kterých je provozována virtualizace VMware vSphere 7. Virtualizační platforma je centrálně spravována přes vCenter 7. Dále je součásti IT infrastruktury centrální diskové pole SAN. Síťová infrastruktura na všech budovách propojených optickými trasami zahrnuje přístupové a core switche[redacted] a dále WiFi přístupové body[redacted] připojené na monitorovací systém [redacted]. [redacted]
Network bude poskytovat data včetně monitoringu síťového provozu. Objednatel si vyhrazuje právo na změnu infrastruktury v průběhu plnění smlouvy a poskytovatel na změny musí neprodleně, nejpozději však do 7 dnů reagovat úpravami konfigurace služby SOC. Zadavatel disponuje ve své infrastruktuře dvěma DNS servery sloužícími pro překlad adres (v případě interních dotazů) a dále využívá DNS server na Ministerstvu vnitra v rámci uzavřené sítě CMS2, který pro zadavatele dělá překlad veškerých dotazů (směřujících do internetu). Kvůli nutnosti zajistit překlady na služby v uzavřené síti CMS2, musí zůstat zajištěno využívání tohoto serveru.

Zdroje	Výrobce	Kusy
HW + VMs Linux servery		40
HW + VMs Windows servery		63

VMs appliance (libovolný OS)		4
Virtualizační nody	[redacted]	4
HW Firewall	[redacted]	2 HA
Switche	[redacted]	39
WiFi AP	[redacted]	104
SAN + NAS	[redacted]	1 + 1
EDR	[redacted]	2 (WS) + 6 (Linux) + cloud
[redacted]	[redacted]	1

V závislosti s případnými změnami i přirozeným vývojem infrastruktury magistrátu města Frýdku-Místku se může množství připojených prvků měnit a tím pádem i množství logů.

2.2 Technické parametry

Předmětem dodávky je komplexní řešení pro centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software provozované formou služby sdíleného dohledového centra kybernetické bezpečnosti SOC. Implementace systému bude provedena v souladu s § 24 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí dle Vyhlášky č. 82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění.

Dále dodávka zahrnuje řešení hlídání a blokace nelegitimních DNS dotazů.

Poskytovatel musí dodat plně funkční řešení dle svých nejlepších znalostí a svědomí, splňující veškeré níže uvedené minimální technické parametry a funkce tak, aby mohl poskytovat službu SOC a hlídání a blokace nelegitimních DNS dotazů.

- Integrovaný systém zpracovávání logů, flow a událostí ze zdrojů definovaných objednatelem
- Pronájem SIEM formou HW appliance
- Implementace HW a SW částí
- Měsíční profylaxe HW a SW částí
- Komunikace týmu poskytovatele se objednatelem v českém nebo slovenském jazyce
- Pravidelná aktualizace software
- Sběr a ukládání logů, flow a událostí ze zdrojů objednatele pro potřeby vyhodnocování s bezpečnostním týmem poskytovatele 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
- [redacted] pro monitoringu síťového provozu (provozováno objednatelem)
- 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 objednatele 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 objednatele Umožnění přístupu do SIEM a dalších systému objednateli s oprávněními pouze pro čtení ve všech částech systému
- Zajištění monitorování zdrojů ve smyslu kontroly dostupnosti
- Podpora pro vzdálené i ruční instalace agentů
- Instalace agentů poskytovatelem
- Zabezpečená replikace všech kybernetických bezpečnostních událostí, alertů a incidentů na federační servery poskytovatele, které jsou umístěny v jeho prostředí
- Veškerá data musí být uložena v datových centrech v Evropské unii, za což zodpovídá poskytovatel
- 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 integrace s MS Active Directory včetně podpory lokálních uživatelů
- Nabízený systém musí integrovat logy, aletry a výstupy z [redacted] objednatele
- Objednatel umožní zaměstnancům poskytovatele přístup do konzole systému Bitdefender, tak aby mohli činit úkony vedoucí k zabránění/rozšíření bezpečnostního incidentu. Tento režim bude na definovaných serverech a bude podléhat změnám dle změn v infrastruktuře objednatele. V současné chvíli jde o 9 serverů
- Zajištění kompletního přehledu o DNS provozu z koncových stanic uživatelů v reálném čase
- Zajištění zabezpečení DNS provozu koncových stanic uživatelů blokací závadných adres s možností kategorizace
- Podporované protokoly systémem SIEM minimálně: snmp, ftp, sftp, netflow, nfs, cifs, syslog
- Zpracovávání průměrně 200–300 EPS, ve špičkách 1000 EPS, v průběhu trvání smlouvy může dojít k nárustu EPS
- Vytvoření kompetenční a komunikační matice
- Vykonávání kybernetického bezpečnostního dohledu v režimu 24x7x365, kdy operátor musí být i v tomto režimu na svém pracovišti (forma pohotovosti není přípustná a objednatel toto může kdykoliv libovolně kontrolovat), zahájení řešení bezpečnostního incidentu, možnost kontaktu poskytovatele objednatelem s žádostí o řešení problému spojeného s poskytovanou službou, s žádostí o konzultaci
- Zasílání SMS zpráv na vybraná tel. čísla na základě vydefinovaných událostí ze 6 zdrojů objednatele (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 je 48 hodin od nahlášení nebo detekce závady (pro tento případ definovat sankce ve smlouvě).
- Jednotné kontaktní místo pro příjem požadavků – service desk, hlášení o kybernetických bezpečnostních incidentech, pro proaktivní komunikaci a pro komunikaci i s třetí stranou (např. NUKIB, NBU, ÚOOÚ, PČR atd.)
- Informování o potvrzeném bezpečnostním incidentu analytikem poskytovatele bezprostředně a neodkladně po jeho zjištění dohodnutou cestou (podpora min. prostřednictvím service desku, emailem, sms, telefonní hovor na tel. čísla dohodnuté v komunikační matici dle priorit a rozsahu)

- V případě detekce kybernetického bezpečnostního incidentu poskytovatel musí garantovat informování operátorem o této skutečnosti nejpozději do 30 min. a zahájení řešení technickým specialistou nejpozději do 2 hod. včetně situace, kdy na kybernetický bezpečnostní incident upozorní objednatel
- Po celou dobu nevyřešeného bezpečnostního incidentu musí poskytovatel poskytnout součinnost při jeho řešení
- Poskytovatel musí poskytnout informaci o detekci kybernetického bezpečnostního incidentu a proaktivní komunikaci o možných řešeních se objednatelem i třetí stranou (např. NUKIB, NBU, ÚOOÚ, PČR atd.)
- Poskytovatel musí objednatele informovat o známých a objevených hrozbách na provozovaných systémech poskytovatele bezprostředně po jejich odhalení
- Jednou za dva měsíce musí poskytovatel provést sken zranitelností v interní infrastruktuře objednatele, nebo na vyžádání, a to v režimu 24x7x365 (se spuštěním skenu do 1 hod.)
- Jednou za dva měsíce musí poskytovatel provést externí sken zranitelností (z internetu)
- Host based sken zranitelností na agentem sledovaných zdrojích (min. Windows a Linux)
- Neprodleně poskytovat informace o únicích informací a dat o doméně a uživatelích objednatele na Dark webu
- 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
- Poskytovatel 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), informace o anomáliích a nestandartním chování v infrastruktuře, např. DNS dotazy na nevydefinované DNS servery, nestandartní protokoly v síti atd. Report musí zahrnovat výstupy ze SIEMu, monitoringu dat a síťového provozu, DNS provozu a skenů zranitelností
- Poskytovatel bude 1x měsíčně s objednatelem procházet a vyhodnocovat měsíční report prostřednictvím online videohovoru v předpokládané délce 1 hod.
- Poskytovatel musí o každé změně v týmu informovat objednatele prostřednictvím emailu na adresu [redacted]

HW/SW komponenta	Nabízený produkt
SIEM	[redacted]
Systém pro monitoring a zabezpečení překladů DNS koncových stanic uživatelů	

2.3 Požadavky na implementaci

- Součástí poskytování služby kybernetického bezpečnostního dohledu bude instalace a implementace veškerých potřebných součástí v místě plnění (Radniční 1148, Frýdek-Místek)
- instalace a konfigurace veškerých SW části
- napojení a konfigurace zdrojů zadavatele na nabízený systém/nabízené systémy
- instalace agentů na zdroje objednatele poskytovatelem
- vypracování a dodání podrobné technické dokumentace podle skutečného nasazení pro zaměstnance odboru IT objednatele v elektronické podobě (ve formátu MS Office 2013 a

vyšší), která musí obsahovat minimálně technický popis řešení, potřebné komunikační porty, popis konfigurace + nastavení a komunikační a kompetenční matici. Technická dokumentace se po předání objednateli 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. Veškeré práce musí probíhat po domluvě se objednatelem.

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

2.4 Harmonogram

Objednatel 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. Poskytovatel 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 objednatele a příprava v místě plnění za přítomnosti zaměstnance objednatele z odboru IT	T + 7 dní (7 dní)
Dodávka nabízeného HW a SW	T + 30 dní (37 dní)
Konfigurace nabízeného HW a SW včetně napojení zdrojů objednatele	T + 14 (51 dní)
Zkušební provoz + školení zaměstnanců objednatele, tvorba dokumentace	T + 7 dní (58 dní)
Předání díla	T + 1 den (59 dní)

Ukončení implementace rozšíření [redacted] bude v předpokládaném termínu k datu 14. 1. 2024. V případě, že bude služba SOC naimplementována a předána v dřívějším termínu, musí dojít následně k donastavení a doimplementování sběru dat a vyhodnocování službou SOC.

2.5 Školení zaměstnanců objednatele

Poskytovatel zajistí školení zaměstnanců objednatele 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