VÝZVA NA PREDLOŽENIE PONUKY (PRIESKUM TRHU)

podľa § 6 ods. 1 zákona č. 343/2015 Z. z. o verejnom obstarávaní

1. Názov predmetu zákazky

SOC - Poskytnutie expertných služieb riadenia incidentov kybernetickej bezpečnosti na účely eliminácie bezpečnostných incidentov (PHZ)

2. Druh zákazky

Poskytnutie služieb

3. Identifikácia verejného obstarávateľa :

Obchodné meno / Názov	Národné centrum zdravotníckych informácií
Poštová adresa	Lazaretská 26, 811 09 Bratislava 1
IČO	00165387
Kontaktná osoba	Katarína Grejták Bednáriková
e-mail	Katarina.GrejtakBednarikova@nczisk.sk
adresa hlavnej stránky verejného obstarávateľa /URL/	www.nczisk.sk
Adresa zadávania zákazky /URL/ v systéme JOSEPHINE	https://josephine.proebiz.com/sk/tender/47386/summary

4. Stručný opis predmetu zákazky

Predmetom prieskumu je získanie indikatívnych cenových ponúk od relevantných hospodárskych subjektov na poskytnutie expertných služieb riadenia incidentov kybernetickej bezpečnosti na účely eliminácie bezpečnostných incidentov v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

5. Spoločný slovník obstarávania

CPV podľa slovníka	Predmet
72000000-5	Služby informačných technológií: konzultácie, vývoj softvéru, internet a podpora
71620000-0	Analytické služby
72220000-3	Systémové a technické poradenstvo
72222000-7	Strategické prehodnotenie a plánovanie informačných systémov alebo technológie
79417000-0	Bezpečnostné poradenstvo

6. Miesto a termín poskytnutia služby:

Rámcová dohoda: **36 mesiacov odo dňa nadobudnutia účinnosti a/alebo do vyčerpania finančného limitu resp. rozsahu rámcovej dohody (podľa toho, ktorá skutočnosť nastane skôr).**

7. Spôsob určenia ceny

(Indikatívna) cena za predmet zákazky musí byť stanovená v zmysle zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov. Navrhovaná cena musí byť v súlade s § 2 citovaného zákona o cenách založená na cene obchodného alebo sprostredkovateľského výkonu, ekonomicky oprávnených nákladoch a primeranom zisku.

Navrhovaná cena musí byť vyjadrená v eurách v súlade so zákonom č. 659/2007 Z. z. o zavedení meny euro v Slovenskej republike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Vyhlášok č. 97/ 2008 Z . z. a 75/2008 Z. z.

Návrh indikatívnej ceny musí obsahovať všetky predpokladané náklady spojené s plnením predmetu zákazky.

Pri tvorbe cenovej ponuky je potrebné zohľadniť aj:
- primeranosť jej stanovenia na základe jemu vzniknutých nákladov a primeranosť zisku,
- požiadavky na technické a odborné kapacity v dostatočnom množstve pre potreby zabezpečenia plnenia predmetu zákazky v požadovaných lehotách a kvalite.

Verejný obstarávateľ požaduje predložiť vyplnenú / nacenenú Prílohu č. 2 tejto výzvy pri zohľadnení opisu predmetu zákazky uvedeného taktiež v Prílohe č. 1.

8. Možnosť predloženia variantných riešení:

Verejný obstarávateľ neumožňuje predložiť variantné riešenia.

9. Lehota na predkladanie ponuky

Lehota na predkladanie indikatívnych cenových ponúk je do: **03.10.2023 do 12.00 hod**.

10. Viazanosť/platnosť ponuky

Min. 3 mesiace odo dňa posledného dňa lehoty na predkladanie indikatívnych cenových ponúk.

11. Platobné podmienky

Platba bude realizovaná formou bezhotovostného platobného styku na základe daňového dokladu vystaveného poskytovateľom, splatnosť ktorého je do 60 kalendárnych dní odo dňa preukázateľného doručenia príslušnej faktúry verejnému obstarávateľovi/objednávateľovi. Verejný obstarávateľ neposkytuje preddavky, ani zálohové platby.

12. Spôsob predloženia indikatívnej ponuky

Prostredníctvom systému Josephine na linke uvedenej v bode 3 tejto výzvy, v prípade výpadku alebo technický problémov výnimočne aj elektronickou poštou na e-mailovú adresu uvedenú v bode 3 tejto výzvy.

13. Ďalšie súvisiace informácie:

Predloženie ponuky je indikatívne a do budúcna nekonštatuje konflikt záujmov a nebráni hospodárskemu subjektu zúčastniť sa zadávania zákazky na vyššie uvedený predmet zákazky po jeho vyhlásení.

Na základe predložených indikatívnych cenových ponúk v prieskume trhu zostaví Národné centrum zdravotníckych informácií ako verejný obstarávateľ v zmysle ZVO predpokladanú hodnotu zákazky, ktorá bude v ďalšom použitá na účely vypracovania analýzy nákladov a prínosov (CBA) pre projekt „Podpora budovania bezpečnostných dohľadových centier v prostredí verejnej správy“ v rámci výzvy MIRRI SR. Predmet zákazky bude v prípade úspešnosti projektu verejného obstarávateľa (spolu)financovaný z prostriedkov Plánu obnovy a odolnosti SR.

V Bratislave, dňa 25.9.2023

Prílohy:

- Príloha č. 1 – Opis predmetu zákazky
- Príloha č. 2 – Štruktúrovaný rozpočet

Príloha č. 1 – Opis predmetu zákazky

Predmetom zákazky je poskytnutie služby pre technické vybavenie formou na vyžiadanie, ktoré predstavujú poskytnutie expertných služieb riadenia incidentov kybernetickej bezpečnosti na účely eliminácie bezpečnostných incidentov v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov počas trvania Rámcovej dohody.

Verejný obstarávateľ preto v oblasti riadenia incidentov kybernetickej bezpečnosti požaduje poskytnutie služby pre technické vybavenie formou na vyžiadanie v nasledovnom rozsahu:

1. služby detekcie a evidencie kybernetických bezpečnostných incidentov prostredníctvom nepretržitého bezpečnostného monitorovania IT prostredia,
2. služby asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov,
3. špecializované služby digitálnych forenzných analýz,
4. špecializované služby testovania a hodnotenia zraniteľnosti informačných systémov prevádzkovaných verejným obstarávateľom,
5. špecializované služby „threat hunting“ a „threat inteligence“,
6. služby asistencie pri riešení kybernetických incidentov na mieste v rozsahu:
    - služieb poradenskej a konzultačnej podpory, vypracovania bezpečnostných politík, koncepcií a návrhu postupov pre riadenie informačnej bezpečnosti v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhláškou č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
    - služieb „business continuity management“ - BCM – a to v rozsahu tvorby procesov pre riadenie kontinuity činnosti upravujúcich postupy, základné zodpovednosti a právomoci pri tvorbe dokumentácie BCM a počas havarijnej situácie,
    - vypracovanie analýz dopadov BIA – a to najmä analytické činnosti na vyhodnotenie dopadov na inštitúciu pri narušení alebo prerušení procesov, určenie kritických procesov a špecifikácií pre ich obnovu, tvorbu a vyhodnocovanie dotazníkov, spracovanie analytických výstupov, prenos spracovaných údajov do plánov,
    - vypracovanie analýzy rizík – najmä analytické činnosti na definovanie a vyhodnotenie rizík pôsobiacich na IKT podporujúce kritické procesy a návrh opatrení na ich eliminovanie alebo zníženie,
    - vypracovanie stratégie kontinuity - najmä vypracovanie návrhov alternatívnych metód na udržanie kontinuity procesov verejného obstarávateľa, návrhov na zaistenie dostupnosti informácií a informačných služieb pre kritické procesy v prípade výskytu havárie,
    - vypracovanie plánov kontinuity činnosti BCP - t. j. alternatívnych postupov na obnovu kritických procesov a IKT po havárii, ktoré budú zahŕňať návrh štruktúry plánov, naviazanie tabuľkových a textových údajov k štruktúre plánov a vytvorenie výstupov,
    - prípravu návrhu a realizácie testov BCP - overenie kvality plánov na základe testovacieho scenára, ktorý zahrňuje výber plánu, personálne zabezpečenie, vyhodnotenie plánu a generovanie správy z testovania,
    - služieb integrácie plánov kontinuity činnosti BCP so systémom bezpečnostného a technologického monitoringu na účely zabezpečenia trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvajúce osobné údaje, ako aj zaistenia

schopnosti včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu.

Verejný obstarávateľ pod pojmom asistencia rozumie realizáciu takých úkonov a činností počas riešenia kybernetických bezpečnostných hrozieb a incidentov, ktoré nevyžadujú priame zásahy do prostredia, kde boli hrozby alebo incidenty odhalené. Asistencia spočíva v kooperácii tímu na strane NCZI a dodávateľa tejto služby, pričom dodávateľ poskytuje expertné služby pre analýzu, odhaľovanie, navrhuje kroky na získanie ďalších podkladov k analýze a navrhuje aj opatrenie na zamedzenie šírenia, zastavenie a odstránenie hrozieb alebo dočasné pozastavenie dotknutých služieb.

Integrálnou súčasťou poskytovania služieb musí byť aj vypracovanie návrhu dokumentácie pre riadenie kybernetickej bezpečnosti v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Riadiaca dokumentácia musí obsahovať minimálne:

- Bezpečnostnú politiku kybernetickej bezpečnosti, ktorá stanoví základné ciele a zodpovednosti v oblasti riadenia identifikácie a riešenia kybernetických bezpečnostných incidentov.
- Klasifikáciu informácií a kategorizáciu sietí a informačných systémov, ktorá pre každú informáciu, sieť a informačný systém stanoví jeho klasifikáciu.
- Smernicu pre riadenie informačnej bezpečnosti, ktorá stanoví základné postupy pre riadenie informačnej bezpečnosti v rozsahu PDCA cyklu v súlade so štandardom STN ISO/IEC 27001:2014 a vyhláškou NBÚ o bezpečnostných opatreniach.
- Smernicu o bezpečnej prevádzke, ktorá ustanoví základné zodpovednosti a povinnosti jednotlivých zamestnancov pre zabezpečenie prevádzky technologickej infraštruktúry v súlade so zákonom o kybernetickej bezpečnosti. Táto smernica musí opisovať relevantné administratívne opatrenia vyplývajúce z analýzy rizík a zákona o kybernetickej bezpečnosti.

Bezpečnostná dokumentácia musí byť vypracovaná pre celú infraštruktúru IKT, aplikačnú architektúru, bezpečnostnú architektúru, implementované bezpečnostné opatrenia, organizačné jednotky v súlade s požiadavkami vyhlášky o bezpečnostných opatreniach pre MZ SR.

Poskytnutie služby pre technické vybavenie formou na vyžiadanie pre zabezpečenie podpory prevádzky a zabezpečenia funkčností CSIRT

Verejný obstarávateľ požaduje poskytnutie služieb pre technické vybavenie formou na vyžiadanie pre riadenie incidentov kybernetickej bezpečnosti v nasledovných oblastiach:

Služba	**Požadované parametre**
Služby detekcie a evidencie kybernetických bezpečnostných incidentov prostredníctvom nepretržitého bezpečnostného monitorovania IT prostredia	definované v bode 1 nižšie
Služby asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov	definované v bode 2 nižšie
Špecializované služby digitálnych forenzných analýz	definované v bode 3 nižšie

Špecializované služby testovania a hodnotenia zraniteľnosti informačných systémov prevádzkovaných verejným obstarávateľom	definované v bode 4 nižšie
Špeciálnych služieb „threat hunting“ a „threat inteligence“	definované v bode 5 nižšie
Služby asistencie pri riešení kybernetických incidentov	definované v bode 6 nižšie

1. Služby detekcie a evidencie kybernetických bezpečnostných incidentov prostredníctvom nepretržitého bezpečnostného monitorovania IT prostredia

Verejný obstarávateľ požaduje na vlastnú zodpovednosť víťazného uchádzača zabezpečiť služby nepretržitého on-line bezpečnostného monitoringu svojich informačných systémov v režime 8x5NBD takým spôsobom, aby bola zaistená dôvernosť, integrita a dostupnosť všetkých komponentov IT infraštruktúry verejného obstarávateľa. Služby nepretržitého bezpečnostného monitoringu musia byť poskytované takým spôsobom, aby bola zaistená prvotná reakcia na vzniknutý incident s prvotnou analýzou príčin vzniku incidentu s jeho popisom a následným vypracovaním návrhov opatrení na elimináciu jeho dopadu na IT infraštruktúru verejného obstarávateľa.

Na účely zabezpečenia kvality požadovaných služieb verejný obstarávateľ definuje nasledovné minimálne požiadavky na kvalitu:

- služba musí realizovať zmenu korelačných pravidiel,
- služba musí poskytovať pravidelné reporty o počte incidentov podľa ich kategorizácie aspoň jedenkrát mesačne,
- služba bezpečnostného monitoringu s garantovanými odozvami na definované incidenty a to nasledovne:

Incident Priority typu 1 (s odozvou do 60 minút) – priorita definuje vysoko nebezpečné incidenty / porušenia pravidiel, ktoré môžu spôsobiť vážne škody v prostredí verejného obstarávateľa. Príklady zahŕňajú kompromitáciu systémov alebo dát, narušenia súkromia; tzv. infikovanie škodlivým kódom alebo jeho šírenie; masívne útoky typu Denial of Service (DoS) alebo Distributed Denial of Service (DDoS); zero day hrozby; vytváranie ID so zvýšenými privilégiami alebo pridanie zvýšených privilégií k existujúcim ID mimo procesov riadenia zmien na strane verejného obstarávateľa; narušenie kritických systémových súborov, aplikačných súborov alebo databáz, ktoré ovplyvnia integritu systému; šírenie škodlivého Software v prostredí verejného obstarávateľa; povolené zmeny politiky;

Incident Priority typu 2 (s odozvou do 12 hodín) – priorita definuje neautorizované aktivity používateľov, ktoré nemajú schopnosť ovplyvňovať výkonnosť systému ani ohroziť dáta verejného obstarávateľa. Medzi príklady tejto priority patrí neoprávnená lokálna skenovacia činnosť; útoky zamerané na konkrétne servery alebo pracovné stanice; neoprávnené vytváranie ID na kritických systémoch; užívateľom spôsobené súvislé neúspešné / úspešné pokusy o prihlásenie; neúspešné pokusy o manipuláciu s kritickými systémami, aplikáciami, záznamovými súbormi a databázami; prístup k kritickým systémom alebo aplikačným súborom; rozšírenie škodlivého kódu ohrozujúceho konkrétny úsek alebo viacero úsekov verejného obstarávateľa.

Incident Priority typu 3 (s odozvou do 24 hodín) – priorita definuje činnosti ako sú bežné chyby užívateľa, nesprávne konfigurácie, nedodržiavanie súladu a skenovanie; tzv. „Discovery scanning“; zhromažďovanie skriptov, iné pokusy o tzv. sondovanie / prieskumy; neoprávnené

reštartovanie systému; používanie účtov (servisných, administrátorských, systémových účtov); aktivity s názvami účtov, ktoré nevyhovujú schváleným štandardom názvov účtov; podozrivé názvy súborov; akékoľvek neoprávnené zmeny alebo aktivity realizované mimo pracovných hodín verejného obstarávateľa; a určité typy výskytu škodlivého kódu

Nevyhnutným predpokladom pre poskytovanie služieb detekcie a evidencie kybernetických bezpečnostných incidentov je zabezpečenie zberu udalostí z dôležitých systémov, zariadení a aplikácií Ministerstva zdravotníctva SR (okrem organizácií v zriaďovateľskej pôsobnosti Ministerstva zdravotníctva) a NCZI. Poskytnutie udalostí z dôležitých systémov je v pôsobnosti IT oddelení organizácií Ministerstva, pričom bude povinnosťou poskytnúť súčinnosť pre túto aktivitu.

Poskytovanie služieb pre technické vybavenie formou na vyžiadanie pre zabezpečenie podpory prevádzky bezpečnostného monitoringu prevádzkovaných informačných systémov v režime 8/5/NBD sa požaduje dodať prostredníctvom nasledovných expertov:

Názov pozície	**Popis požadovaných činností**	**Predpokladaný rozsah**
Služby analytika – vyšetrovateľa Level1	Prvotná reakcia na vzniknutý incident, detekcia a identifikácia incidentu, klasifikácia a prioritizácia incidentu, počiatočná analýza incidentu, komunikácia s dohodnutými zástupcami obstarávateľa ohľadom doplňujúcich informácií o prostredí počas vzniku incidentu, prípadne dodanie dodatočných informácií zo zdrojových systémov, zabezpečenie základného popisu incidentu a krokov, ktoré boli realizované na získanie dodatočných informácií, návrh na nové automatizované mechanizmy identifikácie incidentov.	300 človekodní
Služby analytika – vyšetrovateľa Level2	Detailná analýza incidentu, zabezpečenie detailného popisu incidentu a krokov, ktoré boli realizované na získanie dodatočných informácií, návrh opatrení na elimináciu alebo zníženie dopadu incidentu na chránenú infraštruktúru, návrh opatrení na zamedzenie šírenia incidentu, eskalácia incidentu, tvorba a úprava automatizovaných mechanizmov identifikácie incidentov.	600 človekodní
Služby manažéra SOC	Riadenie kvality a priebehu poskytovaných služieb, rozdeľovanie úloh a riadenie zdrojov pri riešení incidentov, návrh zmien procesov, tvorba a generovanie pravidelných reportov o stave bezpečnosti.	50 človekodní

Služby špecialistu centrálnej bezpečnostnej, logovacej a vyhodnocovacej platformy	Konfigurácia a manažment prevádzkovanej služby, aplikácia opráv a aktualizácií prevádzkovaných služieb, úprava nastavení systému pre zlepšenie výkonu, funkcií, zabezpečenie funkčnosti zberu udalostí zo zdrojových systémov, koordinácia činností so správcami IT prostredia obstarávateľa v prípade riešenia problémov pri zbere.	220 človekodní

Požaduje sa garantovaná dostupnosť služby 8/5/NBD, t.j. 8 hodín 5 dní v týždni s nasledovnými parametrami:

Parametre	**Priorita**		
	1	**2**	**3**
Reakčná doba	60 min	12 hod	24 hod
Doba vypracovania metodiky (runbook) na elimináciu incidentu	1 deň	3 dni	5 dní

Priorita incidentu sa určí na základe nasledovnej matice:

Dopad	Vysoký	3	2	1
	Stredný	3	3	2
	Nízky	3	3	3
		Nízka	Stredná	Vysoká
	Urgencia			

2. Služby asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov

Verejný obstarávateľ poskytnutie služieb pre technické vybavenie formou na vyžiadanie formou asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov požaduje poskytovať prostredníctvom týchto expertov:

Názov pozície	**Popis požadovaných činností**	**Predpokladaný rozsah**

Služby experta pre sieťovú bezpečnosť	Reakcia na vzniknuté incidenty, detailná hĺbková analýza príčin vzniku v oblasti sieťovej bezpečnosti (sieťové a aplikačné FW, analytické systémy, email gateway, proxy), návrh opatrení na zamedzenie dopadu incidentu alebo opatrení na zamedzenie vzniku incidentu, odborná a technická podpora pri riešení vzniknutého incidentu v oblasti sieťovej bezpečnosti (sieťové a aplikačné FW, analytické systémy, email gateway, proxy).	200 človekodní
Služby experta pre bezpečnosť koncových zariadení	Reakcia na vzniknuté incidenty, detailná hĺbková analýza príčin vzniku v oblasti koncových zariadení (Windows, Linux, MacOS), návrh opatrení na zamedzenie dopadu incidentu alebo opatrení na zamedzenie vzniku incidentu, odborná a technická podpora pri riešení vzniknutého incidentu v oblasti koncových zariadení (Windows, Linux, MacOS).	75 človekodní
Služby experta pre databázové systémy	Reakcia na vzniknuté incidenty, detailná hĺbková analýza príčin vzniku v oblasti databázových systémov (Oracle, MS SQL, PostgreSQL), návrh opatrení na zamedzenie dopadu incidentu alebo opatrení na zamedzenie vzniku incidentu, odborná a technická podpora pri riešení vzniknutého incidentu v oblasti databázových systémov (Oracle, MS SQL, PostgreSQL).	75 človekodní
Služby experta pre havarijné plánovanie a obnovu činností	Vypracovanie návrhov plánov kontinuity činnosti, integrácia plánov kontinuity činnosti, pravidelné overovanie kvality plánov na základe testovacieho scenára, výber alternatívnych metód na udržanie kontinuity procesov verejného obstarávateľa, spracovanie návrhu plánov dostupnosti informácií a informačných služieb pre kritické procesy v prípade výskytu havárie	150 človekodní

Verejný obstarávateľ požaduje garantovanú dostupnosť 8/5/NBD, t. j. 8 hodín 5 dní v týždni s nasledovnými parametrami:

Parametre	**Priorita**		
	1	**2**	**3**
Reakčná doba	2 hod	24 hod	48 hod
Doba vypracovania metodiky (runbook) na elimináciu incidentu	1 deň	3 dni	5 dní

Priorita incidentu sa určí na základe nasledovnej matice:

Dopad	Vysoký	3	2	1
	Stredný	3	3	2
	Nízky	3	3	3
		Nízka	Stredná	Vysoká
	Urgencia			

3. Špecializované služby digitálnych forenzných analýz

Služby digitálnych forenzných analýz musia spĺňať požiadavky na bezpečnú akvizíciu a analýzu forenzných dôkazov v celom spektre zdrojových zariadení verejného obstarávateľa. Špeciálne služby forenzných analýz musia byť neoddeliteľnou súčasťou procesu riešenia incidentov a teda softvérové a hardvérové vybavenie pracoviska dodávateľa služieb musí podporovať vykonávanie statickej, dynamickej a behaviorálnej analýzy identifikovaných škodlivých kódov.

Verejný obstarávateľ definuje požiadavky na pracovisko poskytovateľa služieb digitálnych forenzných analýz tak, aby sa uistil že poskytovateľ bude technicky spôsobilý prostredníctvom svojich technických prostriedkov pre mobilnú akvizíciu a preliminárnu analýzu digitálnych dôkazov, technicky zabezpečiť služby „Incident responce team“ aj v „teréne“. Verejný obstarávateľ požaduje poskytnutie služby mobilnej akvizície a analýzy digitálnych forenzných dôkazov tak, aby bol Incident response tím (ďalej tiež „IRT“) z technickej stránky schopný poskytnúť základné IOC priamo na mieste.

V procese forenznej analýzy zastáva extrakcia dôkazov majoritnú a nenahraditeľnú pozíciu. Dostatočné a správne zabezpečenie dôkazov zo zariadenia predstavuje prvý logický a funkčný krok procesu forenznej analýzy, od ktorého závisia všetky následné kroky procesu forenznej analýzy. V rámci reálnych podmienok získavania forenzných dôkazov v mnohých prípadoch dochádza k situácii, kedy je potrebné analyzovať zariadenie, ktoré má prístup chránený autentifikačnými údajmi, alebo sa jedná o poškodené zariadenie, resp. o zariadenie, kde nie je z rozličných príčin možná logická extrakcia dôkazov. V takýchto prípadoch prichádza do úvahy viac menej len fyzická extrakcia a z uvedeného dôvodu musí pracovisko disponovať špecializovaným hardvérovým a softvérovým vybavením pre takýto typ extrakcie forenzných dôkazov. Poskytovanie špeciálnych služieb digitálnych forenzných analýz verejný obstarávateľ požaduje poskytnúť prostredníctvom nasledovného experta:

Názov pozície	**Popis požadovaných činností**	**Predpokladaný rozsah**

Služby experta pre forenznú analýzu	Poskytované činnosti forenznej analýzy musia zahrňovať celý životný cyklus forenznej analýzy od akvizície dôkazov až po záverečnú správu a predstavenie výsledkov pre manažment v nasledovnom rozsahu: a. zariadenia (napr. pracovné stanice, servery, mobilné zariadenia, sieťové prvky atď.) b. sieť, c. dáta a databázy, d. malware, a to ako samostatný proces, alebo ako súčasť procesu riešenia incidentov	100 človekodní

Verejný obstarávateľ požaduje garantovanú dostupnosť 8/5/NBD, t. j. 8 hodín 5 dní v týždni s nasledovnými parametrami:

Parametre	**Priorita**		
	1	**2**	**3**
Reakčná doba	6 hod	24 hod	48 hod

Priorita incidentu sa určí na základe nasledovnej matice:

Dopad	Vysoký	3	2	1
	Stredný	3	3	2
	Nízky	3	3	3
		Nízka	Stredná	Vysoká
	Urgencia			

4. Špecializované služby testovania a hodnotenia zraniteľnosti informačných systémov

Pre zabezpečenie súladu s ustanoveniami § 20 zákona verejný obstarávateľ požaduje poskytnutie služieb pravidelného hodnotenia zraniteľností a penetračného testovania ako integrálnej súčasti pracoviska CSIRT. Súčasťou požadovanej služby musia byť kontinuálne činnosti semiautomatizovaného, resp. automatizovaného vyhľadávania zraniteľností. Verejný obstarávateľ požaduje poskytovať špeciálne služby testovania a hodnotenia zraniteľností informačných systémov prostredníctvom tohto experta:

Názov pozície	**Popis požadovaných činností**	**Predpokladaný rozsah**

Služby experta pre interné penetračné testovanie	Automatizované, semi-automatizované a manuálne vykonávanie penetračných testov z pohľadu a. interného útočníka, b. externého útočníka s fyzickým prístupom do internej siete c. externého útočníka bez fyzického prístupu do siete, v celom rozsahu prostredia vrátane jednotlivých prvkov (napr. penetračné testovanie aplikácií). Služby musia obsahovať vyhľadávanie a hodnotenie zraniteľností ako samostatnú, resp. integrálnu časť penetračných testov.	150 človekodní

5. Špeciálne služby „threat hunting“ a „threat inteligence“

Služby „threat hunting“ a „threat inteligence“ musia zahŕňať minimálne:

- proaktívne vyhľadávanie potencionálnych zraniteľností v prostredí o proaktívne odhaľovanie sofistikovaných foriem útokov, napr. útokov typu APT o návrhy na optimalizáciu monitorovacieho systému
- sledovanie nových typov a foriem hrozieb s následnou kontrolou prostredia na ich možný výskyt
- vytváranie IOCs a návrh na ich implementáciu (napr. ako threat intelligence feed) o poskytovanie návrhov na penetračné testovanie vytipovaných častí prostredia, resp. použitím vytipovaných foriem útokov
- automatické využívanie „threat inteligence“ zdrojov v používaných nástrojoch.

Verejný obstarávateľ požaduje poskytovať špeciálne služby „threat hunting“ a „threat inteligence“ prostredníctvom týchto expertov:

Názov pozície	Popis požadovaných činností	Predpokladaný rozsah
Služby experta pre činnosti „threat hunting“	Všetky činnosti popísané v zozname služieb tejto kapitoly.	150 človekodní
Služby experta pre činnosť využívania „threat inteligence“	Riešenie automatizovaného využívania „threat inteligence“ zdrojov v existujúcich riešeniach zabezpečujúcich predmet zákazky.	75 človekodní

6. Služby asistencie pri riešení kybernetických incidentov

Služby asistencie pri riešení kybernetických incidentov musia poskytnúť jednotke CSIRT centralizovanú správu legislatívnych a normatívnych požiadaviek v oblasti kybernetickej bezpečnosti (ako najmä analýza rizík a posudzovanie súladu). Zabezpečením poskytovania

služieb analýzy rizík (realizovaných v rámci služieb SOC), vyhľadávania zraniteľností a prepojením výsledkov sa musí dosiahnuť komplexný procesne-technický pohľad na aktuálny stav kybernetickej bezpečnosti v sektore „Zdravotníctvo“. Verejný obstarávateľ požaduje poskytnutie služieb v nasledovnom rozsahu:

- poradenskú a konzultačnú podporu pre riadenie kybernetickej bezpečnosti v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti,
- vypracovanie plánov kontinuity činnosti BCP kritických procesov, plány obnovy činnosti a plány reakcie na kybernetické bezpečnostné incident
- poskytnutie podpory pri testovaní plánov kontinuity činnosti, plánov obnovy prevádzky aj plánov reakcie na kybernetické bezpečnostné incidenty s cieľom identifikovať slabé miesta plánov a navrhnúť opatrenia na ich zlepšenie
- vypracovanie analýz dopadov BIA - analytické aktivity zamerané na vyhodnotenie dopadov na inštitúciu pri narušení alebo prerušení procesov, určenie kritických procesov a špecifikácií pre ich obnovu, tvorbu a vyhodnocovanie dotazníkov, spracovanie analytických výstupov, prenos spracovaných údajov do plánov,
- vypracovanie analýzy rizík - analytické aktivity zamerané na definovanie a vyhodnotenie rizík pôsobiacich na IKT podporujúce kritické procesy a návrh opatrení na ich eliminovanie alebo zníženie,
- integrácia plánov kontinuity činnosti BCP so systémom bezpečnostného a technologického monitoringu na účely zabezpečenia trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvajúce osobné údaje, ako aj zaistenia schopnosti včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu.

Verejný obstarávateľ požaduje poskytovať služby asistencie pri riešení kybernetických incidentov prostredníctvom týchto expertov:

Názov pozície	**Popis požadovaných činností**	**Predpokladaný rozsah**
Služby bezpečnostného architekta	Vypracovávanie návrhu architektúr, posudzovanie spôsobu pripájania nových dátových zdrojov prostredníctvom služby prevádzkovanej centrálnou bezpečnostnou, logovacou a vyhodnocovacou platformou, spracovávanie HLD a LLD, poradenská a konzultačná činnosť	75 človekodní
Služby experta pre riadenie informačnej bezpečnosti	Poradenská a konzultačná činnosť a podpora, vypracovanie bezpečnostných politík, koncepcií, návrhu postupov pre riadenie informačnej bezpečnosti	100 človekodní

Príloha č. 2 – Štruktúrovaný rozpočet

P.č.	Názov požadovanej služby/experta	Počet v MD	Jednotková cena za MD v € bez DPH	Celková cena v € bez DPH	Výška DPH	Celková cena v € s DPH
1	Služby analytika – vyšetrovateľa Level1	300,00	€ -	€ -	20%	€ -
2	Služby analytika – vyšetrovateľa Level2	600,00	€ -	€ -	20%	€ -
3	Služby manažéra SOC	120,00	€ -	€ -	20%	€ -
4	Služby špecialistu centrálnej bezpečnostnej, logovacej a vyhodnocovacej platformy	150,00	€ -	€ -	20%	€ -
5	Služby experta pre sieťovú bezpečnosť	200,00	€ -	€ -	20%	€ -
6	Služby experta pre bezpečnosť koncových zariadení	75,00	€ -	€ -	20%	€ -
7	Služby experta pre databázové systémy	75,00	€ -	€ -	20%	€ -
8	Služby experta pre havarijné plánovanie a obnovu činností	150,00	€ -	€ -	20%	€ -
9	Služby experta pre forenznú analýzu	100,00	€ -	€ -	20%	€ -
10	Služby experta pre interné penetračné testovanie	150,00	€ -	€ -	20%	€ -
11	Služby experta pre činnosti „threat hunting“	150,00	€ -	€ -	20%	€ -
12	Služby experta pre činnosť využívania „threat inteligence“	75,00	€ -	€ -	20%	€ -
13	Služby bezpečnostného architekta	75,00	€ -	€ -	20%	€ -
14	Služby experta pre riadenie informačnej bezpečnosti	100,00	€ -	€ -	20%	€ -
SPOLU						**€ -**