Príloha č. 2 **Zoznam, špecifikácia a pravidlá poskytovania Služieb**

Celok 2. Poskytovanie služieb pre technické vybavenie formou na vyžiadanie

prevzaté z ponuky Dodávateľa

Príloha č. 2 Zoznam, špecifikácia a pravidlá poskytovania Služieb

CELOK 2. OPIS PREDMETU ZÁKAZKY O POSKYTOVANÍ SLUŽIEB PRE TECHNICKÉ VYBAVENIE

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

Uchádzač bude poskytovať požadované služby pre technické vybavenie formou na vyžiadanie pre riadenie incidentov kybernetickej bezpečnosti v nasledovných oblastiach:

Služby pre podporu prevádzky a zabezpečenia funkčnosti CSIRT			
Služba	**Požadované parametre**	**ÁNO/NIE**	**Ponuka uchádzača (poznámka)**
Služby detekcie a evidencie kybernetických bezpečnostných incidentov prostredníctvom nepretržitého bezpečnostného monitorovania IT prostredia	definované v kapitole 0	**ÁNO**	**expertný tím**
Služby asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov	definované v kapitole 1.10	**ÁNO**	**expertný tím**
Špecializované služby digitálnych forenzných analýz	definované v kapitole 0	**ÁNO**	**expertný tím**
Špecializované služby testovania a hodnotenia zraniteľnosti informačných systémov prevádzkovaných verejným obstarávateľom	definované v kapitole 0	**ÁNO**	**expertný tím**
Špeciálnych služieb „threat hunting“ a „threat inteligence“	definované v kapitole 0	**ÁNO**	**expertný tím**
Služby asistencie pri riešení kybernetických incidentov	definované v kapitole 0	**ÁNO**	**expertný tím**

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

Uchádzač zabezpečí poskytovanie služieb nepretržitého on-line bezpečnostného monitoringu informačných systémov verejného obstarávateľa v režime 8x5NBD takým spôsobom, aby bola zaistená dôvernosť, integrita a dostupnosť všetkých komponentov IT infraštruktúry verejného obstarávateľa. Služby nepretržitého bezpečnostného monitoringu budú 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 NCZI.

Požadovaná kvalita požadovaných služieb bola verejným obstarávateľom definovaná v nasledovnom rozsahu:

- 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

Poskytovanie služieb pre technické vybavenie formou na vyžiadanie pre zabezpečenie podpory prevádzky bezpečnostného monitoringu prevádzkovaných informačných systémov v režime 8/5/NBD bude uchádzačom dodané expertným tímom nasledovne:

P.č.	Názov pozície	Popis požadovaných činností	Predpokladaný rozsah činností počas trvania Dohody
1.1.	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.	400 človekodní
1.2.	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

1.3.	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.	100 človekodní
1.4.	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.	160 človekodní

Uchádzač garantuje 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 bude určená na základe nasledovnej matice:

Dopad	Vysoký	3	2	1
	Stredný	3	3	2
	Nízky	3	3	3

		Nízka	Stredná	Vysoká
	Urgencia			

1.10. Služby asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov

Uchádzač bude služby pre technické vybavenie formou na vyžiadanie formou asistencie pri riešení kybernetických bezpečnostných hrozieb a incidentov prostredníctvom týchto expertov:

P.č.	Názov pozície	Popis požadovaných činností	Predpokladaný rozsah činností počas trvania Dohody
2.1.	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).	160 človekodní
2.2.	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).	120 človekodní

2.3.	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).	80 človekodní
2.4.	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	40 človekodní

Uchádzač garantuje 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 bude určená na základe nasledovnej matice:

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

Špecializované služby digitálnych forenzných analýz

Služby digitálnych forenzných analýz poskytnuté uchádzačom budú spĺňať požiadavky na bezpečnú akvizíciu a analýzu forenzných dôkazov v celom spektre zdrojových zariadení verejného obstarávateľa. Špeciálne služby forenzných analýz budú 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.

Poskytovanie špeciálnych služieb digitálnych forenzných analýz bude poskytnuté prostredníctvom expertného tímu takto:

P.č.	**Názov pozície**	**Popis požadovaných činností**	**Predpokladaný rozsah činností počas trvania Dohody**
3.1.	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

Uchádzač garantuje dostupnosť služby 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 bude určená na základe nasledovnej matice:

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

Špecializované služby testovania a hodnotenia zraniteľnosti informačných systémov

Uchádzač poskytne služby pravidelného hodnotenia zraniteľností a penetračného testovania ako integrálnej súčasti pracoviska CSIRT. Súčasťou požadovanej služby budú kontinuálne činnosti semi-automatizovaného, resp. automatizovaného vyhľadávania zraniteľností. Uchádzač poskytne špeciálne služby testovania a hodnotenia zraniteľností informačných systémov prostredníctvom experta:

P.č.	Názov pozície	Popis požadovaných činností	Predpokladaný rozsah činností počas trvania Dohody
4.1.	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.	160 človekodní

Špeciálne služby „threat hunting“ a „threat inteligence“

Požadované služby „threat hunting“ a „threat inteligence“ budú zahŕňať:

- proaktívne vyhľadávanie potencionálnych zraniteľností v prostredí
- proaktívne odhaľovanie sofistikovaných foriem útokov, napr. útokov typu APT
- 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)
- poskytovanie návrhov na penetračné testovanie vytipovaných častí prostredia, resp. použitím vytipovaných foriem útokov
- automatické využívanie „threat inteligence“ zdrojov v používaných nástrojoch

Uchádzač bude poskytovať špeciálne služby „threat hunting“ a „threat inteligence“ prostredníctvom expertného tímu takto:

P.č.	Názov pozície	Popis požadovaných činností	Predpokladaný rozsah činností počas trvania Dohody
5.1.	Služby experta pre činnosti „threat hunting“	Všetky činnosti popísané v zozname služieb tejto kapitoly.	160 človekodní
5.2.	Služby experta pre činnosť využívania „threat inteligence“	Riešenie automatizovaného využívania „threat inteligence“ zdrojov v existujúcich riešeniach zabezpečujúcich predmet zákazky.	80 človekodní

Služby asistencie pri riešení kybernetických incidentov

Uchádzačom poskytované služby asistencie pri riešení kybernetických incidentov poskytnú 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 dosiahne komplexný procesne-technický pohľad na aktuálny stav kybernetickej bezpečnosti v sektore „Zdravotníctvo“. Uchádzač poskytne tieto služby v nasledovnom rozsahu:

- poradenská a konzultačná podpora 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.

Služby asistencie pri riešení kybernetických incidentov budú uchádzačom poskytnuté prostredníctvom expertného tímu takto:

P.č.	Názov pozície	Popis požadovaných činností	Predpokladaný rozsah činností počas trvania Dohody
6.1.	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	60 človekodní
6.2.	Služby experta pre riadenie informačnej bezpečnosti	Poradenská a konzultačná činnosť a podpora, vypracovanie bezpečnostných politík, koncepcií, návrhu postupov pre riadenie informačnej bezpečnosti	402 človekodní