1. OBJEDNÁVKA

Zadávací a pověřovací list č. 17/2024

pro Katalogový list č.2 MF_SLV/01

ke Smlouvě o poskytování odborných služeb
uzavřené dne 12. 5. 2020
(evidované u objednatele pod č. 9006/014/2020, č.j. MF-28447/2019/7005)
(evidované u poskytovatele pod ev.č. SML2020026, č.j. SPCSS-02127/2020)

Česká republika – Ministerstvo financí
se sídlem Letenská 15, 118 10 Praha 1
zastoupen: [redacted]
IČO: 00006947
DIČ: CZ00006947
ID datové schránky: xzeaauv
bankovní spojení: [redacted]
číslo účtu: [redacted]
(dále jen „**objednatel**" nebo „**MF**")

a

Státní pokladna Centrum sdílených služeb, s. p.
se sídlem: Na Vápence 915/14, 130 00 Praha 3
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 76922
zastoupený: [redacted]
IČO: 03630919
DIČ: CZ03630919
ID datové schránky: ag5uunk
bankovní spojení: [redacted]
číslo účtu: [redacted]
(dále jen „**poskytovatel**" nebo „**SPCSS**")

Zadání Služby MF_SLV/01, které bude realizovat Poskytovatel podle smlouvy o poskytování odborných služeb (evid. u objednatele pod č. 9006/014/2020 a u poskytovatele pod č. SML2020026).

Služba MF_SLV/01	
Specifikace zadání – název role pro zajištění odborných služeb a informační podpory	3.6 – Specialista bezpečnosti ICT [redacted]
Zadaný počet MD (8 hodin)	maximálně 8,5 MD měsíčně; celkem 51 MD
Období realizace	01.07.2024 – 31.12.2024
Rozsah a popis požadovaných činností	
3.6 Specialista bezpečnosti ICT dle Katalogového listu č.2 MF SLV_01: • prosazuje bezpečnostní strategie a bezpečnostní politiky v rámci resortu MF; • je zodpovědný za implementaci organizačních a technických bezpečnostních rolí do resortu MF; • prosazuje a implementuje pravidla ochrany bezpečnosti informací do řídících projektových struktur při výstavbě IS a ICT resortu MF; • poskytuje metodickou podporu poradnímu orgánu resortu v oblasti bezpečnosti informací a kybernetické bezpečnosti; • navrhuje a překládá plán kontrolní činnosti a harmonogram bezpečnostních auditů, penetračních a zátěžových testů v rámci resortu;	

- provádí vyhodnocování závěrů a dopadů bezpečnostních kontrol, auditů, testů;
- navrhuje opatření pro zvládání bezpečnostních rizik, hrozeb a dopadů;
- účastní se interních, popřípadě externích bezpečnostních auditů, buď na pozici vedoucího interního auditora ISMS nebo jako člena externího auditního týmu;
- vykonává roli Bezpečnostního manažera v projektových týmech, při budování významných informačních systémů nebo kritické komunikační infrastruktury resortu;
- kontroluje soulad prováděných bezpečnostních implementací se schválenými soubory (uživatelskými požadavky na bezpečnost) organizačních a technických opatření v celém životním cyklu projektu, včetně dodržování bezpečnostních pravidel v rámci projektového týmu;
- ve spolupráci s bezpečnostním managementem SOC (Security Operations Center), provádí kontrolu implementace bezpečnostních nástrojů (sond) v prostředí KIS resortu MF;
- poskytuje součinnost při zavádění bezpečnostních opatření do resortu;
- spolupracuje s bezpečnostními architekty jednotlivých informačních a komunikačních systémů resortu na tvorbě architektur, popřípadě při řízení jejich změn;
- poskytuje součinnost při tvorbě systému pro tvorbu a správu aktiv, registru rizik, hrozeb a návrhu jejich eliminace v rámci jednotlivých projektů a v rámci resortu;
- poskytuje součinnost při tvorbě procesů v oblasti sběru logů pro potřeby SIEM, bezpečnostních událostí a incidentů v souladu s požadavky na implementaci systému včasného varování a nastavení systému kybernetické bezpečnosti;
- poskytuje součinnost ostatním resortním týmům SOC a NBÚ v rámci nastavených procesů kybernetické bezpečnosti v resortu MF.

Činnosti spojené s provozem Bezpečnostních produktů SAP na MF

CVA (Code Vulnerability Analysis)

- rozhoduje (či spolurozhoduje – s quality expertem) o výjimkách v procesech schvalování výjimek založených vývojářem.
- koordinuje: analýzy nálezů, návrhů řešení nálezů, realizace opatření z bezpečnostních kontrol CVA (pro zajištění kvality kódu v souladu s pravidly a metodikou IISSP).
- koordinuje běhy bezpečnostních kontrol CVA (termíny, rozsah, ...).
- rozhoduje/spolurozhoduje o dalším postupu nad nálezy z bezpečnostních kontrol CVA.

ETD (Enterprise Thread Detection)

- kontroluje stav (nebo revize řešení) zjištěných událostí, pátrání či výjimek.
- rozhoduje/spolurozhoduje o výjimkách (opodstatněná/neopodstatněná).
- koordinuje nastavení resp. změn režimu generování upozornění na události či výjimky (pro definici příslušných vzorců/patternů a zakládání/řešení pátrání, atd.).
- kontroluje práci administrátorů ETD a jejich vyhodnocení jednotlivých incidentů, nastavení metodik, pravidelná kontrola činnosti adminů.
- rozhoduje/spolurozhoduje o implementaci bezpečnostních patchů.
- kontroluje stav bezpečnostních patchů (průběh/výsledek implementace).

GRC (Governance, Risk and Compliance)

- rozhoduje/spolurozhoduje o požadavcích na přiřazení Firefighterů.
- kontroluje využívání FF (kdo, kdy, proč..).
- koordinuje řešení nálezů z Access Risk Analýzy (pro zajištění „Segregation of duties")

Název role	Cena za MD v Kč bez DPH	Počet MD	Cena za požadovaný počet MD	
			Kč bez DPH	Kč s DPH

3.6 specialista bezpečnosti ICT	20 100,00	8,50	170 850,00	206 728,50
Celkem období realizace 6 měsíců		**51 MD**	**1 025 100,00**	**1 240 371,00**
Specifikace výstupů činností: dle schváleného měsíčního výkazu práce				
Rozsah pověření: v souladu s rozsahem a popisem činností				
Osoby oprávněné za ověření a schválení akceptačních protokolů				
Za objednatele	[redacted]			
Za poskytovatele	[redacted]			
Osoby oprávněné k jednání ve věcech plnění této smlouvy				
Za objednatele	[redacted]			
Za poskytovatele	[redacted]			