

Úrad jadrového dozoru Slovenskej republiky
Bajkalská 1467/27,
820 07 Bratislava – mestská časť Ružinov

v Trenčíne, 11.10.2024

Vec: Žiadosť o vysvetlenie podmienok účasti - stanovisko

Dňa 7.10.2024 sme obdržali žiadosť o vysvetlenie podmienok účasti predložených v ponuke zákazky pod názvom „Podpora, údržba a rozvoj systémov získaných v rámci projektu Zvýšenie úrovne informačnej a kybernetickej bezpečnosti ÚJD SR (zmluva č. 13/2022)“.

Verejný obstarávateľ požiadal o vysvetlenie alebo doplnenie predložených dokladov z dôvodu, že z nich nie je možné posúdiť splnenie požadovaných podmienok účasti:

1. Kľúčový expert č. 2 - Expert pre oblasť sieťovej bezpečnosti – 1 osoba

- minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti implementácie a podpory Fortinet nástrojov, ktoré prevádzkuje verejný obstarávateľ na zabezpečenie sieťovej bezpečnosti.

Verejný obstarávateľ na základe vyššie uvedeného, žiada o bližšie vysvetlenie praktických skúseností uvedených v bode 11 životopisu Petra Ondrejkooviča tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti.

Splnenie požadovanej podmienky účasti sme preukázali poskytovaním odbornej praxi experta p. Ondrejkooviča a to na projektoch

Projekt	odberateľ	činnosť
Správa perimetrových FWs MPLS s	Všeobecná zdravotná poisťovňa, a.s. Panónska cesta 2 851 04 Bratislava	Správa perimetrových FortiGate FWs MPLS s viac ako 10 pobočkami, vyhodnocovanie bezp. hrozieb, pravidelné aplikovanie systémových záplat, troubleshooting pri výpadku služieb. Nastavenie SSO a personalizačných prístupov.
Implementácia bezpečnostnej brány pre mail servery.	Úrad pre dohľad nad zdravotnou starostlivosťou	Implementácia bezpečnostnej brány FortiMail pre mail servery. Konfigurácia FortiGuard IPS a IDS, analýza logov a bezpečnostných rizík. (od 06/2018 návrh, analýza,

		implementácia a správa bezpečnostných informáčných SW a technológií SIEM v súlade so zákonom o KB).
Bezpečnosť MPLS siete.	Úrad geodézie, kartografie a katastra Slovenskej republiky	Garant bezpečnosti MPLS siete s viac ako 10 uzlami v rozsahu návrhu počítačovej siete, implementácie, nasadenia a dohľadu nad IT systémami, aplikácia web aplikačného firewallu FortiWeb pre kataster portál.
Migrácia bezpečnostných politík z Checkpointu a Cisco ASA na Fortigate	Generali Poistovňa, a. s. Lamačská cesta 3/A 841 04 Bratislava	Systémový administrátor linuxových serverov - rhel, ubuntu. Migrácia bezpečnostných politík z Checkpointu a Cisco ASA na Fortigate, nasadenie 2-faktorovej autentifikácie a radiusu pre vzdialený prístup do vnútornej siete, implementácia FortiAP a wifi controllera na centrálu a pobočky. Zabezpečenie webových aplikácií pred útokmi z internetu pomocou WAF, zabezpečenie vysokej dostupnosti pomocou LB.SSO pre webové aplikácie. Troubleshooting a správa bezpečnostných prvkov v sieti. Nasadenie FortiEMS pre viac ako 2000 koncových bodov.

Verejný obstarávateľ požadoval preukázať splnenie podmienky účasti *minimálne dvomi (2) preukázateľnými profesionálnymi praktickými skúsenosťami v oblasti implementácie a podpory Fortinet nástrojov, ktoré prevádzkuje verejný obstarávateľ na zabezpečenie sieťovej bezpečnosti.*

Pod pojmom **Fortinet nástroje** sa rozumie najmä:

- Firewally Fortigate
- Bezpečnostná brána FortiProxy
- WAF Web application firewall FortiWeb
- FortiManager
- FortiGuard

- FortiAnalyzer

Implementácia bezpečnostnej brány pre mail servery bola realizovaná využitím Fortinet nástrojov – a to konkrétne technológiou FortiMail.

Vzhľadom na uvedené je preukázanie použitia produktov a technológií Fortinet nástrojov jednoznačné v požadovanom rozsahu praktických skúseností experta p. Ondrejoviča (napr. Dodatok č. 11 ku zmluve o poskytovaní elektronických komunikačných služieb).

2. Kľúčový expert č. 3 - Expert pre ochranu prevencie dát - 1 osoba

- minimálne 3-ročná preukázateľná odborná prax v oblasti implementácie a podpory nástrojov na zabezpečenie sieťovej bezpečnosti.

Verejný obstarávateľ žiada o bližšie vysvetlenie odbornej praxe uvedenej v životopise Martina Hoju tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti:

- minimálne 3-ročná preukázateľná odborná prax v t. j. konkrétne o bližšie vysvetlenie, ktorou odbornou praxou preukazujete splnenie podmienky účasti týkajúcej sa podpory nástrojov na zabezpečenie sieťovej bezpečnosti.

Splnenie požadovanej podmienky účasti sme preukázali dobou poskytovania služieb účastníkmi na projektoch prax v oblasti implementácie a podpory nástrojov na zabezpečenie sieťovej bezpečnosti.

Expert p. Hojo preukazuje 3-ročnú odbornú prax v oblasti implementácie a podpory nástrojov na zabezpečenie sieťovej bezpečnosti minimálne účasťou na relevantných projektoch a to:

Projekt	odberateľ	činnosť	Čas plnenia
Poskytnutie komplexných služieb pre oblasť kyber bezpečnosti	CellQoS, a.s. Koniarekova 5877/16, 917 01 Trnava IČO: 36817864	Vykonanie analýzy rizík a analýzy dopadov v oblasti informačnej a kyber bezpečnosti , Poskytnutie poradenských a konzultačných služieb pre oblasť kyber bezpečnosti, Dodávka, implementácia a podpora Forcepoint DLP nástrojov na zabezpečenie sieťovej bezpečnosti.	03/2021 – 12/2023
Implementácia bezpečnostných riešení	EMM, spol. s r.o. Sekurisova 16 841 02 Bratislava IČO: 17 316 260	Dodávka a implementácia bezpečnostných riešení Forcepoint DLP Suite pre 1300 užívateľov na 24 mesiacov Vrátane použitia modulu sieťovej bezpečnosti (Forcepoint, Network Discovery).	03/2019 – 05/2021

--	--	--	--

Expert p. Hojo ako kmeňový zamestnanec spoločnosti WDS Solution s. r. o. plnil úlohy v pozícii experta sieťovej bezpečnosti a ochrany dát a poskytoval služby odborníka v oblasti implementácie a podpory nástrojov na zabezpečenie sieťovej bezpečnosti s použitím nástroja Flowmon, čo dokazujeme aj priloženými FA.

Flowmon sa špecializuje na moderné technológie monitorovania sieťovej prevádzky na báze analýzy dátových tokov (NetFlow), na správanie siete (Network Behavior Analysis – NBA) a hardvérovú akceleráciu sieťových komponentov (FPGA). Flowmon tak umožňuje plnú viditeľnosť a bezpečnostnú analýzu sieťovej prevádzky, čo následne uľahčuje detegovať problémy a bezpečnostné incidenty vznikajúce v sieti.

3. Klúčový expert č. 4 - Expert SIEM Riešení - 1 osoba

- *minimálne 3-ročná preukázateľná odborná prax v oblasti implementácií, správy a prevádzky bezpečnostných riešení na centralizované monitorovanie bezpečnosti informačných systémov.* Verejný obstarávateľ na základe vyššie uvedeného, žiada o bližšie vysvetlenie odbornej praxe uvedenej v životopise Igora Ficeka tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti.

Splnenie požadovanej podmienky účasti sme preukázali poskytovaním odbornej praxe v oblasti implementácií, správy a prevádzky bezpečnostných riešení na centralizované monitorovanie bezpečnosti informačných systémov a to minimálne u zamestnávateľa Centrum kybernetickej bezpečnosti, v ktorej expert p. Ficek pracoval od roku 2016 - 2021 t.j. po dobu 5 rokov.

Počas pôsobenia na Centre Kybernetickej Bezpečnosti v rokoch 2016 - 2021 sa p. Ficek intenzívne venoval odborným aktivitám v oblasti implementácie, správy a prevádzky bezpečnostných riešení zameraných na centralizované monitorovanie informačných systémov. Jeho skúsenosti sú rozdelené do niekoľkých kľúčových oblastí, ktoré pokrývajú rôzne aspekty kybernetickej bezpečnosti:

Špecialista SIEM (Security Information and Event Management):

V tejto roli sa zameriaval na návrh, implementáciu a správu SIEM riešení, s cieľom efektívne centrálne monitorovať a analyzovať bezpečnostné udalosti. Jeho úlohou bolo zabezpečiť, aby SIEM platforma efektívne zbierala a korelovala bezpečnostné logy z rôznych zdrojov a poskytovala včasné varovania o bezpečnostných incidentoch.

Budovanie a správa CSIRT a SOC tímu:

Ako člen a neskôr vedúci tímu CSIRT (Computer Security Incident Response Team) a SOC (Security Operations Center) sa podieľal na implementácii a koordinácii procesov zameraných na centralizované monitorovanie IS, detekciu a reakciu na bezpečnostné incidenty. Získal

skúsenosti v oblasti technického riadenia incident handlingu, ktoré sa zaoberá detekciou a mitigáciou bezpečnostných hrozieb.

Analýza a implementácia bezpečnostných riešení:

Jeho prax zahŕňa hĺbkovú analýzu požiadaviek na bezpečnostný monitoring a návrh riešení, ktoré zohľadňujú jedinečné potreby a zraniteľnosti informačných systémov našich klientov. Riešenia, ktoré implementoval, zahŕňali aj konfiguráciu nástrojov na ochranu pred bezpečnostnými hrozbami, zlepšenie logovania a nastavenie detekčných a reakčných mechanizmov.

Návrh architektúry a implementácia SIEM:

V spomínanom období mal možnosť pracovať na návrhu a implementácii architektúry SIEM, ktorá zabezpečuje nielen centralizované monitorovanie, ale aj koreláciu udalostí a škálovateľnosť systému. Okrem návrhu samotnej architektúry som vykonával aj technickú konfiguráciu a testovanie riešenia, aby sa dosiahla čo najvyššia účinnosť pri odhaľovaní potenciálnych bezpečnostných incidentov.

Na základe získaných poznatkov a praktických skúseností expert p. Ficek následne úspešne realizoval viacero projektov v oblasti implementácie a správy bezpečnostného centrálneho monitorovania IS a incident manažmentu. Tieto projekty zahŕňali komplexné návrhy a implementácie riešení na mieru, ktoré umožnili našim klientom efektívne monitorovať, detegovať a riešiť bezpečnostné hrozby. Jeho odbornosť v tejto oblasti mu umožnila nielen participovať na budovaní centrálneho monitoringu KB ICT, ale aj efektívne riadiť bezpečnostný tím expertov a koordinovať ich činnosť v súlade s osvedčenými postupmi v oblasti kybernetickej bezpečnosti.

Uvedené skutočnosti potvrdzujeme aj praktickými skúsenosťami poskytnutými v rámci projektov uvedených v odborných skúsenostiach (napr. Projekt: Komplexné riešenie centrálneho manažmentu, Projekt: Zvýšenie kybernetickej bezpečnosti (ďalej tiež „KB“) informačných technológií v správe a užívaní SSC a pod).

4. Kľúčový expert č. 5 - Expert pre systém pre riadenie prístupov zo vzdialených sietí - 1 osoba

- minimálne 3-ročná preukázateľná odborná prax v oblasti implementácií, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM),

Verejný obstarávateľ na základe vyššie uvedeného, žiada o bližšie vysvetlenie odbornej praxe uvedenej v životopise Ondreja Kováča tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti.

Splnenie požadovanej podmienky účasti sme preukázali dobou poskytovaní účasťami na projektoch v oblasti implementácií, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM),

Expert p. Kováč preukazuje 3-ročnú odbornú prax v oblasti implementácií, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM) minimálne účasťou na relevantných projektoch a to:

Projekt	odberateľ	činnosť	Čas plnenia
Inovácia sieťovej infraštruktúry	eGroup Solutions, a.s. Plynárenská 7/B 821 09 Bratislava - mestská časť Ružinov IČO: 44989709	Implementácia Cyberark PAM a zavádzanie SIEM v spoločnosti UJD, a.s. /v postavení subdodávateľa/	03/2023 – 04/2024
Konzultácie nasadenia a rozšírenia riešení riadenia privilegovaných účtov	Transpetrol a.s. Šumavská 38, Bratislava IČO:31341977	Konzultácie nasadenia a rozšírenia riešení riadenia privilegovaných účtov s nástrojom CyberArk,	10/2021 – 02/2022
Implementácia správy riadenia	ČSOB SK	Implementácia správy riadenia privilegovaných účtov s nástrojom CyberArk Správa a prevádzka bezpečnostných riešení pre riadenie prístupov zo vzdialených sietí	01/2015 – 10/2020
AITEN SAP CLOUD	Aiten a.s. Bajkalská 19B, 82101 Bratislava IČO: 36221945	Implementácia CyberArk PAM a zavádzanie SIEM na zabezpečenie sieťovej bezpečnosti Podpora CyberArk nástrojov na zabezpečenie sieťovej bezpečnosti	6/2023 – 1/2024

Na základe uvedeného máme za preukázané, že expert p. Kováč reálne poskytoval služby v oblasti implementácií, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM) a to od roku 2015 až doteraz.

Spoločnosť ALISON Slovakia s.r.o. po tom, ako uspela v zákazke vyhlásenej spoločnosťou ČSOB SK posilnila svoj realizačný tím odborníkov a prijala v septembri 2015 do zamestnania p. Kováča ako experta v oblasti v oblasti implementácií, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM).

Potvrdzujeme, že expert p. Kováč počas obdobia v rozsahu od 09/2015 do ukončenia projektu 10/2020 sa podieľal na implementácii, správy a prevádzky bezpečnostných riešení pre riadenie prístupov (PAM) počas tohto obdobia na danom projekte.

5. Kľúčový expert č. 6 - Expert pre systém pre zabezpečenie životného cyklu bezpečnostného informačného systému - 1 osoba

- *minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v implementácii kontroly a podpory informačných systémov.*

Verejný obstarávateľ na základe vyššie uvedeného žiada o bližšie vysvetlenie praktických skúseností uvedených v životopise Martina Orema tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti:

Splnenie požadovanej podmienky účasti sme preukázali účasťami experta p. Orema na relevantných projektoch, ktoré boli realizované v prospech spoločnosti DXC Technology Slovakia s. r. o., Galvaniho 7, Bratislava.

Projekt Manažment osobných údajov bol realizovaný v období 4/2023 do 12/2023 a to súbežne s projektom Rozvoj platformy integrácie údajov v období 8/2023 – 12/2023.

Ako je zrejmé, projekt Manažment osobných údajov bol realizovaný ako „pilotný“ a prioritne v tomto projekte bola realizovaná okrem iného aj implementácia kontroly a podpory informačných systémov pre zavedenie platformy MOU, nastavenia a jej začlenenia do bezpečnostnej infraštruktúry (viď osvedčenie o realizácii služieb).

Hodnovernosť horeuvedených skutočností si môžu členovia komisie verejného obstarávateľa overiť u osôb zodpovedných za kontrolu realizácie diela a jeho odovzdanie v súlade so Zmluvou o dielo č. 13/2022 zo dňa 8.6.2022 ak aj u osôb pracovníkov odberateľa u ktorých je možné tieto údaje overiť.

S pozdravom

M

Ing. Lukáš Bumbál
konateľ spoločnosti

