MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY

Sekcia verejného obstarávania
Odbor pre zadávanie nadlimitných zákaziek
Štefanovičova 5, 817 82 Bratislava 15

Všetkým záujemcom

Vaše číslo/zo dňa	Naše číslo	Vybavuje/tel.	Bratislava
	MF/015391/2025-273 050649/2025	Ing. Uhnáková/02-5958 4007	23 12. 2025

Vec
Vysvetlenie informácií potrebných na vypracovanie ponuky – č. 4

Na základe doručenej žiadosti o vysvetlenie informácií potrebných na vypracovanie ponuky a v súlade s § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“ alebo „ZVO“ alebo „zákon o verejnom obstarávaní“) verejný obstarávateľ poskytuje vysvetlenie informácií potrebných na vypracovanie ponuky k verejnej súťaži na predmet zákazky **„Posilnenie informačnej a kybernetickej bezpečnosti MF SR**“, ktorá bola vyhlásená vo Vestníku EÚ č. 223/2025 dňa 19. 11. 2025 pod zn. 765368-2025 a vo Vestníku verejného obstarávania č. 234/2025 dňa 20. 11. 2025 pod zn. 18386 - MSS.

I. Otázky záujemcu

Všeobecne:

V súlade s § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“) Vás žiadame o bezodkladné vysvetlenie neprimeraných a potenciálne diskriminačných požiadaviek uvedených v Prílohe č. 6 – Podmienky účasti, časť 2.3.3 "Minimálna požadovaná úroveň štandardov".

Verejný obstarávateľ požaduje, aby experti spĺňali mimoriadne široké, vysoko špecializované a navzájom nesúvisiace certifikačné a skúsenostné požiadavky, vrátane:

- CISSP / CISA / CASP+,
- OSCP, GPEN, GXPN, CEH (penetračné testovanie),
- CHFI, GCFE, GCFA (digitálna forenzná analýza),
- dlhoročnej praxe v APT Incident Response a pôsobenia ako Incident Commander,
- 5-ročnej praxe v oblasti forensic analysis a threat intelligence,
- projektových certifikácií PRINCE2, SCRUM, SAFE, PM².

Dovoľujeme si upozorniť, že uvedené certifikácie a odborné predpoklady sa týkajú najmä činností, ktoré sú typické pre:

CERT/CSIRT tímy,

- digitálnu forenznú analýzu (DFIR),
- pokročilé red teaming/penetration testing aktivity
- threat intelligence,
- incident handling pri APT útokoch.

Naopak, podľa Prílohy č. 1 a Prílohy č. 10 predmet zákazky pozostáva najmä z:

- návrhu a implementácie SOC infraštruktúry,

- inštalácie HW a SW komponentov,
- konfigurácie Fortinet, VMware, RHEL, Windows Server, Veeam a Elastic Stack,
- analýzy IT infraštruktúry a identifikácie attack surface,
- vykonania základných vulnerability scanov,
- návrhu detekčných pravidiel na základe MITRE ATT&CK,
- dodania dokumentácie.

V súťažných podkladoch nie je uvedená žiadna aktivita, ktorá by vyžadovala:

- penetračné testovanie,
- digitálnu forenznú analýzu,
- threat intelligence služby,
- riešenie APT incidentov,
- úlohu Incident Commandera,
- red teaming činnosti.

TABUĽKA NESÚLADU – Požadované certifikácie vs. reálne aktivity projektu

Expert	Požiadavky VO	Aktivity v projekte	Relevancia
Expert 1 – bezpečnostný architekt	CISSP, CASP+, TOGAF/ArchiMate, PRINCE2/SCRUM	návrh DNR, architektúra SOC	CISSP/PRINCE2 → neprimerané, nesúvisiace
Expert 2 – IR/Forensics/Pentest špecialista	OSCP, GPEN, GXPN, CEH, CHFI, GCFE, GCFA, APT IR Commander, Threat Intel, Forensics	projekt neobsahuje IR/DFIR/pentest/TI	80 % požiadaviek nesúvisí s predmetom zákazky
Expert 3 – SOC špecialista	CySA+, SIEM/ELK prax	tvorba use-cases, SIEM konfigurácia	prevažne relevantné; 5 rokov IR → nadmerné

Najmä požiadavky na Experta č. 2 sú úplne mimo rozsahu predmetu zákazky, keďže projekt podľa dokumentácie:

- NEobsahuje žiadne penetračné testovanie,
- NEobsahuje žiadne forenzné analýzy,
- NEobsahuje žiadne incident response služby,
- NEobsahuje žiadnu APT alebo DFIR činnosť.

Podľa ust. § 10 ods. 1 ZVO: *„Verejný obstarávateľ a obstarávateľ sú povinní pri zadávaní zákaziek, koncesií a pri súťaži návrhov postupovať podľa tohto zákona.“*
Podľa ust. § 10 ods. 2 ZVO: *„Verejný obstarávateľ a obstarávateľ musia dodržať princíp rovnakého zaobchádzania, princíp nediskriminácie hospodárskych subjektov, princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti.“*
Podľa ust. § 38 ods. 5 ZVO: *„Podmienky účasti, ktoré verejný obstarávateľ a obstarávateľ určia na preukázanie splnenia finančného a ekonomického postavenia a technickej spôsobilosti alebo odbornej spôsobilosti, musia byť primerané a musia súvisieť s predmetom zákazky alebo koncesie. Verejný obstarávateľ a obstarávateľ môžu vyžadovať od uchádzačov alebo od záujemcov minimálnu úroveň finančného a ekonomického postavenia alebo technickej spôsobilosti alebo odbornej spôsobilosti.“*
V intenciách vyššie citovaných ustanovení § 10 a 38 ZVO je možné konštatovať, že zákonodarca kladie dôraz na zásadu primeranosti, ktorá predstavuje základnú zásadu pre zabezpečenie fungujúceho vnútorného trhu EÚ. V tejto súvislosti si dovoľujeme poukázať na rozhodnutie SD EÚ C 148/15 Parkinson für die Grundfreiheiten182, v ktorom SD EÚ uviedol: „Hoci cieľ zabezpečiť bezpečné a kvalitné zásobovania liekmi na celom vnútroštátnom území v zásade vychádza z článku 36 ZFEÚ, platí pritom, že právna úprava, ktorá môže obmedziť základnú slobodu zaručenú Zmluvou, ako je voľný pohyb tovaru, môže byť platne odôvodnená len vtedy, ak je spôsobilá zaručiť uskutočnenie sledovaného legitímneho cieľa a nejde nad

rámec toho, čo je nevyhnutné na jeho dosiahnutie (pozri v tomto zmysle rozsudky z 9. decembra 2010, Humanplasma, C-421/09, EU:C:2010:760, bod 34, ako aj z 23. decembra 2015, Scotch Whisky Association a i., C-333/14, EU:C:2015:845, bod 33).183“
V kontexte pravidiel zadávania verejných zákaziek sa zásada primeranosti uplatňuje okrem iného aj pri stanovení podmienok účasti podľa ust. § 38 ods. 5 ZVO, nakoľko tieto by mali súvisieť s predmetom zákazky a nemali by prekračovať nároky kladené na uchádzača, ktoré sú nevyhnutné pre riadne plnenie predmetu zákazky. Súvislosť podmienok účasti s predmetom zákazky predstavuje parameter, ktorý vylučuje situácie, kedy skúsenosti kľúčového odborníka nie sú potrebné na plnenie predmetu zákazky. V konkrétnom prípade skúsenosti a certifikácia kľúčových odborníkov pre digitálnu forenznú analýzu (DFIR), pokročilé red teaming/penetration testing aktivity, threat intelligence, incident handling pri APT útokoch neovplyvňujú schopnosť uchádzača riadne dodať predmet plnenia:

- návrh a implementácia SOC infraštruktúry,
- inštalácia HW a SW komponentov,
- konfigurácia Fortinet, VMware, RHEL, Windows Server, Veeam a Elastic Stack,
- analýza IT infraštruktúry a identifikácie attack surface,
- vykonanie základných vulnerability scanov,
- návrh detekčných pravidiel na základe MITRE ATT&CK,
- dodanie dokumentácie.

V tejto súvislosti si dovoľujeme si poukázať na rozhodnutie Rady ÚVO č. 7002- 9000/2021 zo dňa 24. 09. 2021:
„V kontexte uvedených skutočností úrad poukazuje na Rozhodnutie rady úradu č. 7002- 9000/2021 zo dňa 24. 09. 2021 kde rada úradu v bode 66.skonštatovala nasledovné, cit.: „Úrad však zároveň v tejto súvislosti správne konštatoval, že verejný obstarávateľ je povinný stanoviť podmienky účasti v súlade s § 38 ods. 5 zákona o verejnom obstarávaní, pričom určením podmienok účasti vo verejnom obstarávaní verejný obstarávateľ nemôže bezdôvodne obmedziť okruh potenciálnych dodávateľov, ale musí umožniť rovnaké príležitosti všetkým potenciálnym dodávateľom, ktorí sú schopní predmet zákazky plniť (...). Ako už bolo uvedené, aj keď stanovenie podmienok účasti bude vždy znamenať istú formu obmedzenia pre potenciálnych uchádzačov, ktorí stanovené podmienky účasti nebudú spĺňať, je nevyhnutné, aby boli podmienky účasti nastavené primerane vo vzťahu k veľkosti, zložitosti a technickej náročnosti konkrétnej zákazky, a aby bezdôvodne nezvýhodňovali určité hospodárske subjekty, pričom zároveň platí, že podmienky účasti nesmú ísť nad rámec toho, čo je potrebné na dosiahnutie cieľa.“
Zásada proporcionality kladie dôraz na to, aby spôsoby verejného obstarávania, ktoré verejný obstarávateľ zvolil, zodpovedali osobitostiam a dôležitosti príslušného predmetu zákazky.
V tejto súvislosti si dovoľujeme poukázať na metodické usmernenie úradu č. 14436-5000/2024 z 04.11.2024 „V rozhodnutí úradu č. 4939-6000/2021 v spojení s rozhodnutím rady úradu 7002- 9000/2021 sa uvádza , cit.: „...účelom stanovenia podmienok účasti vo verejnom obstarávaní je overiť si postavenie záujemcu, resp. uchádzača z hľadiska osobného postavenia, finančného a ekonomického postavenia alebo technickej alebo odbornej spôsobilosti, čím sa verejný obstarávateľ ubezpečí, že plnenie zmluvy bude zabezpečované spôsobilým zmluvným partnerom v požadovanom rozsahu a kvalite. Je preto logické, že stanovenie podmienok účasti bude vždy znamenať istú formu obmedzenia, nakoľko nie je možné od verejných obstarávateľov požadovať, aby nimi stanovené podmienky účasti mali na všetkých potenciálnych záujemcov rovnaký dopad, t. j. aby stanovené podmienky účasti spĺňal automaticky každý záujemca. Takáto požiadavka by navyše nebola ani možná a bola by v rozpore so samotným účelom inštitútu podmienok účasti ako takého, ktorého účelom je zaistiť práve to, aby ponuku predložili len takí uchádzači, ktorí sú spôsobilí realizovať predmet zákazky. Úrad ďalej uviedol, že verejný obstarávateľ prostredníctvom stanovenia podmienok účasti týkajúcich sa technickej alebo odbornej spôsobilosti eliminuje z účasti na procese verejného obstarávania na daný predmet zákazky tých záujemcov alebo uchádzačov, u ktorých nie je vzhľadom na rozsah ich predchádzajúcich skúseností a výsledkov ich doterajšej podnikateľskej činnosti dôvodné predpokladať, že daný predmet zákazky budú najmä z technického hľadiska schopní dodať, poskytnúť, či uskutočniť riadne a v súlade so stanovenými obchodnými podmienkami. Úrad mal teda za to, že samotným účelom inštitútu podmienok účasti je nastavenie pravidiel, ktoré umožňujú preskúmať spôsobilosť uchádzačov alebo záujemcov s cieľom umožniť súperenie o zákazku iba spôsobilým hospodárskym subjektom, u ktorých existuje predpoklad riadneho plnenia zákazky.“ (...) „Verejný obstarávateľ alebo obstarávateľ môže od uchádzačov v zmysle ustanovenia § 42 ods. 10 zákona o verejnom

obstarávaní vyžadovať skúšobný protokol alebo osvedčenie vydané orgánom posudzovania zhody, či už v rámci opisu predmetu zákazky, v kritériách na vyhodnotenie ponúk alebo v zmluvných podmienkach. V zmysle § 10 ods. 2 zákona o verejnom obstarávaní aj táto požiadavka by mala byť stanovená v súlade so základnými princípmi verejného obstarávania. Vychádzajúc z princípu proporcionality verejní obstarávatelia by nemali prekračovali hranice toho, čo je vhodné a potrebné na dosiahnutie sledovaných cieľov. Tým sa rozumie, že v prípade, ak existuje voľba medzi viacerými primeranými opatreniami, je potrebné prikloniť sa k tomu najmenej obmedzujúcemu, pričom spôsobené ťažkosti nesmú byť neúmerné vo vzťahu k sledovaným cieľom. Na správnu aplikáciu tohto princípu je teda nevyhnutné poznať cieľ, ku ktorému má konanie verejného obstarávateľa smerovať. Ak k danému cieľu vedie viacero možných ciest, verejný obstarávateľ alebo obstarávateľ sa v zásade má prikloniť k tej najmenej obmedzujúcej pre hospodárske subjekty vo verejnom obstarávaní. Máme za to, že v každom prípade má byť verejný obstarávateľ alebo obstarávateľ schopný svoje požiadavky na preukázanie podmienky účasti alebo požiadavky na predmet zákazky jasne a preskúmateľne odôvodniť, a tieto požiadavky by mali byť, ako uvádzame vyššie, primerané a mali by súvisieť s predmetom zákazky. V texte vašej žiadosti sa pri uvádzaných požiadavkách verejného obstarávateľa na predloženie dokladov a informácií nenachádzajú žiadne dôvody akokoľvek odôvodňujúce ich potrebu, primeranosť či nevyhnutnú súvislosť s predmetom zákazky a ani z iných zdrojov nám takéto informácie nie sú známe. Ak si myslíte, že požiadavky verejného obstarávateľa alebo obstarávateľa sú neprimerané alebo odporujúce základným princípom verejného obstarávania a v dôsledku nich dochádza k umelému zúženiu hospodárskej súťaže, dávame do pozornosti možnosť uplatnenia revíznych postupov v zmysle šiestej časti, štvrtej hlavy zákona o verejnom obstarávaní."

Zároveň ÚVO v rozhodnutí č. 6788-6000/2023-OD/4 z 23.08.2023 uviedol:

„Z hľadiska základných princípov verejného obstarávania uvedených v § 10 ods. 2 zákona o verejnom obstarávaní, ako aj v súlade s § 38 zákona o verejnom obstarávaní musia byť podmienky účasti nediskriminačné, transparentné, jasné, primerané a opodstatnené vo vzťahu k predmetu zákazky. Posudzovať primeranosť úrovne stanovených podmienok účasti kontrolovaným je vždy potrebné vo vzťahu k charakteru, náročnosti, významu a účelu predmetu zákazky so zreteľom na všetky uvedené okolnosti."

Napokon si dovoľujeme poukázať na rozhodnutie Rady ÚVO č. 15727-9000/2019 zo dňa 26. 04. 2023 (citované v prehľade rozhodnutí ÚVO za 17. týždeň 2023):

„Rada preto skonštatovala, že ak v predmetnom prípade kontrolovaný nepreukázal nevyhnutnosť (a teda ani primeranosť) ním určených podmienok účasti, ktoré vo výraznej miere limitujú okruh hospodárskych subjektov, ktorým je umožnené uchádzať sa o danú zákazku (čo zhodne vyplýva z tvrdení navrhovateľa, kontrolovaného, ako aj zo záverov odborníčky), záujem kontrolovaného nemôže úplne prevážiť nad záujmom zabezpečiť, aby verejné obstarávanie bolo otvorené hospodárskej súťaži (efektívnej konkurencii)."

V nadväznosti na vyššie citovanú rozhodovaciu prax ÚVO si dovoľujeme uviesť, že zásady verejného obstarávania sú navzájom prepojené a vytvárajú jeden kompaktný celok. Napríklad princíp primeranosti predpokladá stanovenie podmienok účasti tak, aby tieto zabezpečovali riadne plnenie predmetu zákazky a neprekračovali jeho rámec. V prípade stanovenia podmienok účasti, ktoré prekračujú mieru nevyhnutnosti, dochádza k zúženiu hospodárskej súťaže tak, že iba minimum hospodárskych subjektov (spravidla jeden) tieto podmienky splní. Zúženie hospodárskej súťaže na minimum hospodárskych subjektov predstavuje vylúčenie konkurencie v takej intenzite, že táto má vplyv aj na hospodárnosť nakladania s verejnými zdrojmi, nakoľko uchádzač, ktorý bude spĺňať neprimerane stanovené podmienky účasti, nebude pod konkurenčným tlakom, ktorý by mal vplyv na cenotvorbu pri príprave ponuky.

Neprimerane stanovené podmienky účasti zároveň vytvárajú aj predpoklad pre nehospodárne nakladanie s verejnými prostriedkami, nakoľko tieto budú smerovať na financovanie kľúčových odborníkov, ktorých skúsenosti prekračujú rámec predmetu zákazky, čo môže predstavovať rovnako aj porušenie finančnej disciplíny podľa rozpočtových pravidiel verejnej správy a porušenie povinností pri správe cudzieho majetku.

Primeranosť podmienok účasti predstavuje požiadavku na také schopnosti uchádzačov, ktoré budú postačujúce na riadne plnenie predmetu zákazky. Neprimerane sú stanovené v prípade, ak intenzita požadovaných skúseností uchádzačov/kľúčových odborníkov prekračuje predmet zákazky – napríklad,

v prípade realizácie opravy cesty II. triedy by sa vyžadovala skúsenosť s opravou diaľnice, alebo by verejný obstarávateľ v prípade zákazky v hodnote 500.000,- EUR na opravu cesty prvej triedy vyžadoval skúsenosť uchádzača/kľúčového odborníka realizáciou podobného projektu za 1.000.000,- EUR. Stanovená podmienka účasti je síce neprimeraná (a z uvedeného dôvodu by bola predurčená na zrušenie postupu zadávania zákazky po otvorení ponúk), aspoň vykazuje súvislosť s predmetom zákazky.

V tejto súvislosti si dovoľujeme poukázať aj na metodiku ÚVO – zhrnutie najčastejších porušení k stanoveniu podmienok účasti – „Rovnako je verejný obstarávateľ a obstarávateľ povinný v súlade s § 32 ods. 6 zákona o verejnom obstarávaní vymedziť požiadavky na preukázanie finančného a ekonomického postavenia a technickej alebo odbornej spôsobilosti len na tie, ktoré bezprostredne súvisia s rozsahom, zložitosťou a charakterom predmetu zákazky, čo neznamená len priamu vecnú súvislosť s predmetom zákazky, ale i adekvátnosť rozsahu požiadaviek verejného obstarávateľa a obstarávateľ, t. j. ich primeranosť." (...) „Úrad dáva do pozornosti aj stanovenie ďalšej diskriminačnej podmienky, ktorá spočívala v požiadavke, aby garant projektu dosiahol VŠ vzdelanie III. stupňa, pričom verejný obstarávateľ žiadnym spôsobom danú požiadavku nedokázal zdôvodniť. Úrad má za to, že dosiahnutý III. stupeň vysokoškolského vzdelania (navyše bez uvedenia oblasti, v ktorej má byť dané vysokoškolské vzdelanie dosiahnuté) automaticky nepredisponuje osobu disponujúcu takýmto vzdelaním na uspokojivejšie splnenie predmetu zákazky. Naopak, subjekty s osobami, ktoré nedosiahli III. stupeň vysokoškolského vzdelania sú stanovením takejto požiadavky zo strany verejného obstarávateľa neopodstatnene diskriminované, čo je v rozpore s princípom nediskriminácie vo verejnom obstarávaní podľa § 9 ods. 3 zákona o verejnom obstarávaní. Vzhľadom na vyššie uvedené skutočnosti považoval úrad podmienku účasti týkajúcu sa vysokoškolského vzdelania III. stupňa pre garanta projektu za nesúvisiacu s predmetom zákazky, a teda aj v rozpore s § 32 ods. 6 zákona o verejnom obstarávaní a súčasne aj za diskriminačnú."

V prípade predmetnej zákazky však neexistuje žiadna súvislosť medzi podmienkami účasti -skúsenosťami a certifikáciou kľúčových odborníkov pre digitálnu forenznú analýzu (DFIR), pokročilé red teaming/penetration testing aktivity, threat intelligence, incident handling pri APT útokoch s predmetom zákazky:

- návrh a implementácia SOC infraštruktúry,
- inštalácia HW a SW komponentov,
- konfigurácia Fortinet, VMware, RHEL, Windows Server, Veeam a Elastic Stack,
- analýza IT infraštruktúry a identifikácie attack surface,
- vykonanie základných vulnerability scanov,
- návrh detekčných pravidiel na základe MITRE ATT&CK,
- dodanie dokumentácie.

Zároveň prax a certifikácia pre digitálnu forenznú analýzu (DFIR), pokročilé red teaming/penetration testing aktivity, threat intelligence, incident handling pri APT útokoch automaticky neznamená, že kľúčový odborník bude vedieť plniť predmet zákazky

- návrh a implementácie SOC infraštruktúry,
- inštalácia HW a SW komponentov,
- konfigurácia Fortinet, VMware, RHEL, Windows Server, Veeam a Elastic Stack,
- analýza IT infraštruktúry a identifikácie attack surface,
- vykonanie základných vulnerability scanov,
- návrh detekčných pravidiel na základe MITRE ATT&CK,
- dodanie dokumentácie.

V kontexte vyššie uvedeného považujeme požiadavku na skúsenosti a certifikáciu kľúcového odborníka pre digitálnu forenznú analýzu (DFIR), pokročilé red teaming/penetration testing aktivity, threat intelligence, incident handling pri APT útokoch za neopodstatnenú diskrimináciu.

Pre úplnosť dodávame, že v súťažných podkladoch nie je uvedené ani odôvodnenie primeranosti, z ktorého by vyplývala súvislosť stanovených podmienok účasti s predmetom zákazky.

Požiadavky na expertov, najmä pre Experta č. 2:

- nesúvisia s predmetom zákazky,
- sú neprimerané,
- sú technicky neodôvodniteľné,
- nie sú nevyhnutné na plnenie,
- a majú zjavne obmedzujúci vplyv na hospodársku súťaž.

Takáto kombinácia exkluzívnych certifikácií a skúseností je prakticky nesplniteľná drvivou väčšinou hospodárskych subjektov na relevantnom trhu SR/EÚ.

Pre úplnosť dodávame, že po otvorení ponúk už nebude možné neprimerané podmienky účasti zmeniť inak ako zrušením postupu zadávania zákazky a vyhlásením nového verejného obstarávania.

Otázka č. 1

V odpovediach na ŽoV č. 1 verejný obstarávateľ uvádza, že analýza prístupových infraštruktúr zahŕňa:
- identifikáciu dostupných služieb z externého prostredia,
- základné techniky enumerácie,
- vykonanie vulnerability scanov,
- zhodnotenie možností útokov.

Tieto činnosti predstavujú technický audit a identifikáciu zraniteľností, nie aktívne penetračné testovanie, exploitation ani post-exploitation.

Ako verejný obstarávateľ odôvodňuje požiadavku na certifikácie OSCP, GPEN, GXPN alebo CEH, ktoré sú určené pre aktívne penetračné testovanie a exploitation techniky, keď predmet zákazky neobsahuje žiadne penetračné testy ani činnosti charakteru red teamingu?

Otázka č. 2

V odpovediach na ŽoV ani v Prílohe č. 1 a č. 10 nie je uvedené, že projekt zahŕňa:
- digitálnu forenznú analýzu,
- analýzu artefaktov, pamäťových dumpov alebo obrazov diskov,
- rekonstrukciu útokov,
- analýzu škodlivého kódu,
- IR procesy v rozsahu CSIRT/CERT tímov.

Projekt pozostáva z implementácie a konfigurácie technológií, analýzy IT infraštruktúry, identifikácie attack surface a tvorby detekčných pravidiel.
Na základe čoho verejný obstarávateľ považuje požiadavky na CHFI, GCFE alebo GCFA za primerané a nevyhnutné, keď predmet zákazky neobsahuje forenzné služby ani DFIR aktivity?

Otázka č. 3

Verejný obstarávateľ vo svojich odpovediach ani raz neuvádza:
- že súčasťou projektu je riešenie kybernetických incidentov,
- že dodávateľ má vykonávať IR služby,
- že má dochádzať k vyšetrovaniu útokov,
- že má dochádzať k APT huntingu alebo APT mitigation scenárom.

Ako verejný obstarávateľ odôvodňuje požiadavku, aby Expert č. 2 preukázal vedenie závažných APT incidentov ako Incident Commander, keď takáto činnosť nie je súčasťou predmetu zákazky ani nie je uvedená v žiadnej technickej špecifikácii?

Otázka č. 4

Príloha č. 1 definuje analýzu attack surface ako identifikáciu rizík a zraniteľností na úrovni externých služieb, cloudových rozhraní a sociálneho/ fyzického priestoru. V špecifikáciách ani v odpovediach na ŽoV nie je uvedené:

- spracovanie TI feedov,
- tvorba TI reportov,
- korelácia globálnych hrozieb,
- threat hunting činnosti.

Na základe čoho verejný obstarávateľ požaduje 5-ročnú prax v oblasti threat intelligence, keď TI nie je definovaná ako požadovaná činnosť, výstup ani služba v predmete zákazky?

Otázka č. 5

Expert č. 2 musí podľa Prílohy č. 6 spĺňať súčasne:

- IR certifikácie,
- DFIR certifikácie,
- red-team/pentest certifikácie,
- 5 rokov praxe v threat intelligence,
- 5 rokov praxe v digitálnej forenzike,
- 5 rokov incident response,
- prax Incident Commandera pri APT útokoch.

Ide o špecializácie, ktoré sa bežne vykonávajú v samostatných tímoch (CSIRT, DFIR, Red Team, TI) a na trhu sa nevyskytujú v jednej osobe.

Ako verejný obstarávateľ odôvodňuje primeranosť takejto kumulácie požiadaviek v jednej expertnej pozícii podľa § 34 ods. 3 zákona?

Otázka č. 6

Keďže podľa technickej špecifikácie aj odpovedí na ŽoV predmet zákazky pozostáva najmä z:

- implementácie HW/SW,
- konfigurácie technológií,
- analýzy aktív,
- identifikácie attack surface,
- návrhu detekčných pravidiel,

a neobsahuje IR/DFIR/TI/pentest služby,

ako verejný obstarávateľ zabezpečil, aby požadované certifikácie a prax pre expertov neobmedzovali hospodársku súťaž v zmysle § 10 zákona a aby podmienky účasti boli primerané predmetu zákazky podľa § 34 ods. 3 zákona?

Otázka č. 7

Plánuje verejný obstarávateľ upraviť podmienky účasti pre expertov tak, aby zodpovedali reálnemu rozsahu činností definovaných v Prílohe č. 1 a č. 10 a aby nevyžadovali nadmerné certifikácie a skúsenosti, ktoré nesúvisia s predmetom zákazky?

II. Odpoveď verejného obstarávateľa

Všeobecne:

Verejný obstarávateľ považuje za potrebné v úvode zdôrazniť, že predmetom tohto verejného obstarávania nie je izolovaná dodávka technológií ani čiastková implementácia vybraných softvérových alebo hardvérových komponentov, ale **komplexné dielo**, ktorého výsledkom má byť **funkčné, architektonicky konzistentné a prevádzkyschopné Security Operations Center (SOC)** ako integrálna súčasť **oddelenia CSIRT MF SR**.

Účelom budovaného diela je zabezpečiť **kontinuálne poskytovanie služieb kybernetickej bezpečnosti** pre širšiu konštituenciu rezortných organizácií MF SR, a to najmä v prostredí informačných systémov, ktoré **podporujú kritické procesy financovania štátu**. Z uvedeného dôvodu má výsledné riešenie zabezpečiť primeranú úroveň ochrany, včasnú detekciu bezpečnostných udalostí, ich koreláciu, vyhodnocovanie a podporu rýchlej a koordinovanej reakcie na bezpečnostné incidenty.

Z tohto východiska vyplýva, že verejný obstarávateľ pri stanovení podmienok účasti podľa § 34 zákona o verejnom obstarávaní postupoval v súlade s ustálenou rozhodovacou praxou Úradu pre verejné obstarávanie, podľa ktorej musia byť podmienky účasti **vecne, funkčne a logicky prepojené s predmetom zákazky**, primerané jej rozsahu, povahe a významu a nesmú mať diskriminačný charakter. Požadované znalostné štandardy preto neboli stanovené formálne, ale s cieľom zabezpečiť, aby úspešný uchádzač disponoval reálnou odbornou kapacitou na návrh, integráciu a uvedenie do prevádzky SOC riešenia ako operačnej schopnosti CSIRT.

Verejný obstarávateľ v tejto súvislosti poukazuje na skutočnosť, že v rámci projektu „Zvyšovanie úrovne informačnej a kybernetickej bezpečnosti MF SR“ boli uplatnené porovnateľné znalostné a certifikačné požiadavky na kľúčových expertov. Aktuálne stanovené znalostné štandardy v Prílohe č. 6 súťažných podkladov na tieto požiadavky **nadväzujú**, avšak zároveň reflektujú **objektívny posun v rozsahu, pôsobnosti a význame poskytovaných služieb**.

Na rozdiel od predchádzajúceho projektu je SOC v tomto prípade koncipovaný ako **centrálna bezpečnostná kapacita CSIRT MF SR**, ktorá zabezpečuje služby pre širšiu konštituenciu rezortných organizácií. Tomu zodpovedá aj **zvýšenie nárokov na kompetenčné schopnosti expertov**, keďže sa rozširuje rozsah chránených informačných systémov, ich kritickosť a potenciálny dopad kybernetických bezpečnostných incidentov na chod štátu.

Verejný obstarávateľ pri stanovovaní znalostných štandardov zohľadnil aj **kritickú úlohu informačných systémov, ktorých ochrana a monitorovanie budú zabezpečované prostredníctvom budovaného SOC**, najmä v oblasti riadenia štátneho dlhu, likvidity a realizácie finančných operácií štátu.

Tieto informačné systémy tvoria **základný predpoklad schopnosti štátu plniť svoje finančné záväzky**, zabezpečovať plynulé financovanie verejných politík a udržiavať dôveryhodnosť Slovenskej republiky na finančných trhoch. V prípade ich znefunkčnenia alebo významného obmedzenia by mohlo dôjsť najmä k strate schopnosti operatívne riadiť hotovostnú pozíciu štátu a plánovať peňažné toky, obmedzeniu alebo znemožneniu obsluhy štátneho dlhu, vrátane úhrad úrokov a splátok záväzkov, narušeniu vyrovnávania záväzkov štátu voči domácim aj zahraničným subjektom a sekundárnym dopadom na stabilitu verejných financií a dôveru investorov.

Osobitnú pozornosť verejný obstarávateľ venuje aj **potenciálnym dôsledkom výpadku alebo kompromitácie systémov štátnej pokladnice**, ako aj súvisiacich platobných a zúčtovacích mechanizmov. Takýto stav by mohol viesť k dočasnému pozastaveniu realizácie platieb štátu, omeškaniu plnenia finančných záväzkov voči verejným inštitúciám, dodávateľom a občanom a k vážnemu narušeniu kontinuity poskytovania základných verejných služieb.

V prípade dotknutia sa systémov zabezpečujúcich **medzinárodný platobný styk**, vrátane rozhraní na globálne finančné siete (napr. SWIFT), by sa tieto dopady mohli **preniesť aj do medzinárodného prostredia**, s potenciálnym reputačným a finančným dosahom presahujúcim vnútroštátny rámec.

Zároveň verejný obstarávateľ uvádza, že kybernetická bezpečnosť v oblasti financií a bankovníctva sa odlišuje od kybernetickej bezpečnosti v iných sektoroch najmä rozsahom rizík, okamžitým dopadom incidentov a regulatornými nárokmi, ktoré sú na tieto prostredia kladené. Ide o oblasť, kde kybernetické incidenty nemajú len technický alebo prevádzkový charakter, ale bezprostredne ovplyvňujú finančnú stabilitu, dôveru v štát a fungovanie ekonomiky. Finančný sektor je dlhodobo jedným z primárnych cieľov sofistikovaných kybernetických útokov organizovaného kybernetického zločinu a v niektorých prípadoch štátom podporovaných aktérov a APT skupín. Toto kladie zvýšené nároky na expertov, ktorí musia rozumieť pokročilým útočným technikám, detekcii anomálií a korelácii udalostí.
Verejný obstarávateľ zároveň považuje za nevyhnutné zdôrazniť, že predmet zákazky predstavuje **jeden funkčný celok**, t. j. súbor vzájomne prepojených technických, procesných a organizačných prvkov, ktoré sú navrhnuté, implementované a integrované tak, aby ako celok plnili svoju primárnu funkciu – **včasnú detekciu, vyhodnotenie a podporu riešenia kybernetických bezpečnostných incidentov** v prostredí informačných systémov s vysokou mierou kritickosti.

Funkčným celkom sa v tomto kontexte rozumie infraštruktúra SOC pozostávajúca z hardvérových a softvérových komponentov, bezpečnostného monitoringu, logovania, korelácie udalostí, detekčných mechanizmov, procesných väzieb a integračných rozhraní, ktoré musia fungovať koordinovane a spoľahlivo aj v prípade závažných bezpečnostných incidentov. Zlyhanie alebo nevhodný návrh ktorejkoľvek z týchto častí môže mať priamy negatívny dopad na schopnosť štátu reagovať na kybernetické hrozby a útoky.

Z uvedeného dôvodu musí byť návrh tohto diela realizovaný **starostlivo, odborne a s prihliadnutím na reálne skúsenosti z praxe**, a nie výlučne na základe teoretických znalostí alebo izolovaných technických konfigurácií. Verejný obstarávateľ preto pri stanovení znalostných štandardov vychádzal z:

- vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti,
- European Cybersecurity Skills Framework (ECSF),
- ako aj z vlastných praktických skúseností nadobudnutých pri prevádzke SOC a pri realizácii predchádzajúceho projektu „Zvyšovanie úrovne informačnej a kybernetickej bezpečnosti MFSR“.

Tieto rámce a skúsenosti jednoznačne poukazujú na potrebu **súhry viacerých odborných znalostí**, ktoré sa v reálnom prostredí SOC prirodzene prelínajú – od porozumenia hrozbám a správania útočníkov, cez analýzu bezpečnostných udalostí, až po návrh detekčných mechanizmov a architektúry bezpečnostného monitoringu. Verejný obstarávateľ preto pristúpil k výberu znalostných štandardov tak, aby zohľadňovali túto komplexnosť a zabezpečili, že návrh riešenia bude vychádzať z prakticky overených prístupov a osvedčených postupov.

Cieľom verejného obstarávateľa nie je požadovať nadbytočné alebo nesúvisiace kvalifikácie, ale zabezpečiť, aby dodávateľ disponoval odborným tímom, ktorý dokáže navrhnúť a realizovať funkčný, stabilný a dlhodobo udržateľný systém SOC. Práve **vzájomná súhra starostlivo a odborne vybraných znalostí a skúseností** je kľúčovým predpokladom na dodanie diela, ktoré bude plnohodnotne využiteľné v prevádzke a schopné reagovať na dynamicky sa meniace kybernetické hrozby.

Verejný obstarávateľ preto považuje za nevyhnutné, aby návrh, konfigurácia a integrácia SOC riešenia boli realizované odborníkmi s preukázateľnými skúsenosťami a znalosťami v oblasti riadenia, riešenia a predchádzania bezpečnostných incidentov a návrhu bezpečnostných architektúr s vysokými nárokmi na dostupnosť, integritu a odolnosť. Tieto zvýšené požiadavky predstavujú **primeranú a odôvodnenú reakciu na rozšírenie pôsobnosti CSIRT MF SR, rastúcu kritickosť chránených systémov** a vysvetľujú rozdiel oproti znalostným štandardom uplatneným v predchádzajúcom projekte.

Verejný obstarávateľ pri stanovení znalostných štandardov zároveň postupoval s mimoriadnou odbornou starostlivosťou aj s ohľadom na **výrazný vývoj kybernetických hrozieb v posledných rokoch**, nárast sofistikovaných útokov a reálne incidenty s významným spoločenským a prevádzkovým dopadom **(napr. Kybernetický útok na Úrad geodézie, kartografie a katastra SR z januára 2025)**. Tieto okolnosti preukázali, že kybernetické bezpečnostné incidenty môžu zásadným spôsobom ohroziť kontinuitu poskytovania verejných služieb. Z tohto dôvodu považuje verejný obstarávateľ za primerané, aby súčasťou požadovaných odborných kapacít boli aj kompetencie súvisiace s **riadením bezpečnostných incidentov (incident commander)**, a to nie za účelom výkonu samotného incident response v rámci projektu, ale za účelom návrhu SOC riešenia, ktoré je na takéto situácie pripravené.

Požadované znalostné štandardy expertov zároveň bezprostredne súvisia s činnosťami, ktoré budú v rámci projektu vykonávané, vrátane **analýz prístupových infraštruktúr rezortných organizácií**, ich bezpečnostnej architektúry, návrhu segmentácie, logovania, korelácie udalostí a reakčných scenárov. Tieto činnosti si vyžadujú skúsenosti s bezpečnostnými incidentmi, forenzným pohľadom na dáta a pochopením reálnych scenárov hrozieb v heterogénnych prostrediach.

Verejný obstarávateľ uvádza, že predmetné verejné obstarávanie je uverejnené vo Vestníku Európskej únie, čím je zabezpečená možnosť účasti hospodárskych subjektov z celého vnútorného trhu Európskej únie. **Na tomto trhu existuje dostatočný počet odborníkov spĺňajúcich požadované znalostné štandardy, čo potvrdili aj výsledky predbežných trhových konzultácií. Oslovené subjekty v rámci týchto konzultácií potvrdili realizovateľnosť predmetu zákazky, ako aj schopnosť zabezpečiť expertov s požadovanými znalosťami.** Verejný obstarávateľ zároveň zdôrazňuje, že požadované znalosti je možné preukázať aj prostredníctvom viacerých fyzických osôb, a preto nastavené podmienky účasti nemožno považovať za diskriminačné ani neprimerané.

Verejný obstarávateľ nižšie uvádza odpovede na otázky kladené v rámci žiadosti o vysvetlenie:

Odpoveď na otázku č. 1:

Verejný obstarávateľ predpokladá, že otázka vychádza z interpretácie, že požadované činnosti v oblasti analýzy prístupových infraštruktúr predstavujú výlučne formálny technický audit bez potreby hlbších znalostí útočných techník. Verejný obstarávateľ si dovoľuje preto rozsah a účel týchto činností bližšie vysvetliť.
Predmetom verejného obstarávania je poskytovanie služieb v oblasti analýzy informačnej a kybernetickej bezpečnosti v prístupových infraštruktúrach verejného obstarávateľa, a to prostredníctvom posúdenia ich súladu s požiadavkami vyplývajúcimi zo zákona o kybernetickej bezpečnosti, zákona o ITVS a ich vykonávacích predpisov. Súčasťou týchto služieb je aj vykonanie technického auditu, ktorý však nie je chápaný len ako pasívna kontrola konfigurácií alebo dokumentácie, ale ako odborné posúdenie reálneho vystavenia infraštruktúr voči možným útokom.

Ako je uvedené v opise predmetu zákazky, technický audit zahŕňa okrem analýzy IT architektúry a inventarizácie aktív aj analýzu tzv. attack surface, ktorej cieľom je identifikovať všetky relevantné miesta, kde by útočník mohol získať prístup do infraštruktúry. Táto analýza zahŕňa digitálny, fyzický aj sociálny attack surface a jej súčasťou je identifikácia verejne dostupných služieb, portov, aplikácií a rozhraní, vykonanie techník na zistenie dostupných služieb z externého prostredia, realizácia vulnerability skenov a odborné zhodnotenie možností útokov vyplývajúcich z identifikovaných zraniteľností a konfigurácií.

Verejný obstarávateľ ***zdôrazňuje, že odborné a zodpovedné zhodnotenie možností útokov nie je možné bez hlbokej znalosti útočných techník, postupov a reálnych scenárov zneužitia.***

Požadované certifikácie ako OSCP, GPEN, GXPN alebo CEH sú preto stanovené za účelom objektívneho a overiteľného spôsobu preukázania odborných znalostí v oblasti fungovania útokov, techník prieniku a reálneho zneužívania zraniteľností. Práve tieto znalosti sú nevyhnutné na to, aby expert vedel správne interpretovať výsledky vulnerability skenov, rozlíšiť teoretickú zraniteľnosť od prakticky zneužiteľnej, posúdiť pravdepodobnosť a dopad možného útoku v konkrétnom kontexte infraštruktúry a navrhnúť adekvátne bezpečnostné opatrenia a odporúčania.

Bez takejto znalostnej bázy by analýza možností útokov zostala len na deklaratívnej alebo formálnej úrovni, bez reálneho prínosu pre zvyšovanie bezpečnosti prístupových infraštruktúr verejného obstarávateľa.

Verejný obstarávateľ zároveň zdôrazňuje, že požadované certifikácie sú uvedené alternatívne, nie kumulatívne, a slúžia ako jeden z viacerých spôsobov preukázania odborných znalostí. Ich cieľom nie je obmedziť hospodársku súťaž, ale zabezpečiť, aby analýzy vykonávali odborníci, ktorí rozumejú útočnému pohľadu („attacker mindset") a sú schopní kvalifikovane posúdiť riziká vyplývajúce z reálneho vystavenia infraštruktúr voči hrozbám.

Na záver verejný obstarávateľ uvádza, že požiadavky na znalostné štandardy sú stanovené v súlade s rozsahom a významom predmetu zákazky, reflektujú charakter analyzovaných prístupových infraštruktúr a sledujú legitímny cieľ zabezpečenia primeranej úrovne ochrany informačných systémov verejného obstarávateľa v súlade s platnou legislatívou.

Odpoveď na otázku č. 2:

Verejný obstarávateľ berie na vedomie otázku uchádzača, ktorá vychádza z užšieho výkladu rozsahu činností explicitne pomenovaných v opise predmetu zákazky. Verejný obstarávateľ zároveň považuje za potrebné uviesť, že predmet zákazky je koncipovaný ako ***komplexné dielo****, ktorého cieľom je návrh a implementácia bezpečnostného riešenia SOC ako jedného funkčného celku, a nie ako súbor izolovaných služieb striktne vymedzených názvom jednotlivých odborných disciplín.*

Požiadavky na certifikácie ako CHFI, GCFE alebo GCFA preto slúžia ako ***objektívne overiteľný nástroj preukázania odborných znalostí a praktických skúseností****, ktoré sú nevyhnutné na kvalifikovaný návrh detekčných mechanizmov, správnu interpretáciu bezpečnostných udalostí, pochopenie možných dopadov incidentov a návrh architektúry riešenia tak, aby bolo použiteľné aj v prípade reálnych bezpečnostných incidentov.*

Ako je uvedené v Prílohe č. 1 – Opis predmetu zákazky, predmet zákazky zahŕňa komplexný súbor analytických a návrhových činností, na základe ktorých má byť navrhnuté a nakonfigurované bezpečnostné monitorovanie prístupových infraštruktúr verejného obstarávateľa. Výstupy týchto analýz tvoria priamy podklad pre návrh implementácie bezpečnostného monitoringu pozostávajúceho z produktov dodávaných v rámci tohto projektu.

Na základe výsledkov analýzy existujúcej IT infraštruktúry, jej bezpečnostného stavu a analýzy tzv. attack surface (v digitálnej, fyzickej aj sociálnej rovine) bude realizovaný návrh detekčných pravidiel vyplývajúcich z definovaných prípadov použitia (use cases), a to najmä nasledovnými spôsobmi:

- *Use cases vychádzajúce z MITRE ATT&CK Framework-u, pri ktorých sa na základe informácií o IT infraštruktúre prístupovej lokality identifikujú relevantné techniky a taktiky útokov. Pre tieto use cases sa následne navrhujú konkrétne detekčné pravidlá a vhodné produkty dodávané v rámci projektu, v ktorých budú tieto pravidlá optimálne vyhodnocované. Pri tomto návrhu je požadované pokrytie minimálne jedného use case pre každú taktiku uvedenú v rámci „Enterprise tactics", s výnimkou taktík, ktoré nie je možné monitorovať z dôvodu ich realizácie výlučne na strane útočníka. Pri tomto type use cases nejde len o pozapínanie vstavaných use cases vychádzajúcich z MITRE ATT&CK. Ide o dôkladnú analýzu potreby spúšťať len tie, ktoré sú nevyhnutne potrebné ako aj zabezpečenie zberu potrebných logov. Zároveň aj o určenie technológie, ktorá je najvyhovujúcejšia daný use case monitorovať. Nie je cieľom mať spustené detekčné pravidlá, ktoré v konečnom dôsledku nemajú šancu detegovať podozrivé aktivity z rôznych príčin ako nedostatočnosť logov, chybná konfigurácia prípadne zle vytvorené výnimky.*
- *Use cases vytvorené na základe výsledkov analýzy attack surface jednotlivých prístupových infraštruktúr, ktoré reflektujú reálne vystavenie infraštruktúry možným útokom, používané technológie, ich konfiguráciu a vzájomnú integráciu.*
- *Use cases definované na základe špecifických požiadaviek vlastníkov kritických aktív, kde sa v spolupráci s vlastníkmi aktív klasifikovaných ako kritické identifikujú vysoko rizikové aktivity, ktoré*

je nevyhnutné monitorovať a pri ich detekcii overovať legitimitu ich vykonania. Očakávaný počet takto definovaných use cases je približne 50.

Na základe navrhnutých use cases a z nich vyplývajúcich detekčných pravidiel je ďalej požadované navrhnutie logovacieho štandardu, ktorý určuje rozsah, typ a štruktúru logov potrebných na zabezpečenie funkčnosti navrhnutých detekčných pravidiel a korelačných mechanizmov.
Uvedené činnosti si vyžadujú, aby expert disponoval hlbokým porozumením tomu, aké technické artefakty, systémové udalosti a dátové stopy vznikajú v dôsledku bezpečnostných incidentov a techník útokov, a ako sú tieto stopy využiteľné pri detekcii, korelácii a vyhodnocovaní bezpečnostných udalostí.
Práve tieto znalosti sú predmetom certifikácií z oblasti digitálnej forenznej analýzy a DFIR, a sú nevyhnutné pre návrh efektívneho a prakticky použiteľného SOC monitoringu, aj keď samotný výkon forenzných analýz nie je predmetom tohto obstarávania.

Ide najmä o pochopenie vzťahu medzi správaním útočníka a vznikom logov, systémových udalostí a indikátorov kompromitácie, schopnosť posúdiť, či navrhované logovanie a monitoring poskytujú dostatočné podklady pre identifikáciu a analýzu incidentov, návrh architektúry zberu, uchovávania a ochrany bezpečnostných dát tak, aby boli použiteľné aj v prípade potreby hlbšej analýzy incidentu zo strany CSIRT MF SR.

*Znalosti preukazované certifikáciami CHFI, GCFE alebo GCFA sú v tomto kontexte relevantné nie preto, že by sa v rámci projektu vykonávala digitálna forenzná analýza, ale preto, že tieto certifikácie overujú **hlboké porozumenie správania systémov pri bezpečnostných incidentoch**, práce s dátami vznikajúcimi počas incidentov a vzťahu medzi útokom a jeho technickými prejavmi v infraštruktúre.*

*Bez takéhoto porozumenia by návrh SOC riešenia, detekčných pravidiel a monitorovacích scenárov zostal na formálnej úrovni a nemusel by zabezpečiť požadovanú úroveň použiteľnosti riešenia v reálnej prevádzke. Verejný obstarávateľ pritom výslovne požaduje, aby budované SOC riešenie bolo **funkčné, prevádzkyschopné a pripravené na podporu riešenia bezpečnostných incidentov**, aj keď samotné riešenie incidentov nie je predmetom tohto obstarávania. Verejný obstarávateľ sa potrebuje s mimoriadnou dôverou spoľahnúť na funkčnosť dodávaného diela, na ktorom bude závisieť riešenie kybernetických bezpečnostných incidentoch v prostredí s mimoriadnou citlivosťou na diskontinuitu služieb.*

*Verejný obstarávateľ zároveň zdôrazňuje, že požadované certifikácie sú stanovené **alternatívne**, nie kumulatívne, a predstavujú len jeden zo spôsobov preukázania odbornej spôsobilosti experta. Ich cieľom nie je zužovať hospodársku súťaž, ale zabezpečiť, aby návrh a konfigurácia SOC infraštruktúry vychádzali z reálneho pochopenia bezpečnostných incidentov a ich technických dopadov na systémy.*

Na záver verejný obstarávateľ uvádza, že požiadavky na certifikácie CHFI, GCFE alebo GCFA sú primerané rozsahu a charakteru predmetu zákazky, sú v priamej väzbe na činnosti definované v Prílohe č. 1. Verejný obstarávateľ zdôrazňuje, že práve tieto znalosti umožňujú expertom správne prepájať výstupy analýzy aktív, identifikácie attack surface a návrhu detekčných pravidiel s reálnymi scenármi útokov a ich dôsledkami v prevádzke. Bez takéhoto odborného zázemia by existovalo zvýšené riziko návrhu riešenia, ktoré by síce formálne spĺňalo technické požiadavky, avšak nebolo by plnohodnotne využiteľné v praxi CSIRT/SOC tímu verejného obstarávateľa.

Odpoveď na otázku č. 3:

*Verejný obstarávateľ považuje za potrebné uviesť, že **opis predmetu zákazky vymedzuje rozsah požadovaných výstupov a činností**, avšak **nemôže a ani nemá ambíciu vyčerpávajúcim spôsobom popísať všetky odborné predpoklady, ktoré majú vplyv na kvalitu a použiteľnosť výsledného diela**.*
Práve z tohto dôvodu zákon o verejnom obstarávaní rozlišuje medzi opisom predmetu zákazky a podmienkami účasti, ktorých účelom je zabezpečiť, aby uchádzač disponoval odbornou spôsobilosťou primeranou povahe a významu zákazky.
*Verejný obstarávateľ zdôrazňuje, že podmienky účasti sú jedným z nástrojov, prostredníctvom ktorých sa **nepriamo zabezpečuje kvalita výsledného diela**, a to najmä pri projektoch s vysokou mierou odbornosti*

a kritickým dopadom. Skúsenosti Incident Commandera so závažnými APT incidentmi majú priamy vplyv na kvalitu návrhu SOC riešenia.
Verejný obstarávateľ zároveň uvádza, že v prílohe č. 6 – Podmienky účasti ***nie je požadovaný výlučne odborník so skúsenosťami s riadením incidentov spôsobených APT skupinami****, ako je to v otázke prezentované. Požadované sú skúsenosti za posledných 5 rokov v oblasti riešenia závažných kybernetických bezpečnostných incidentov, pričom týmito závažnými kybernetickými bezpečnostnými incidentami sa chápe:*

- *incidenty s vplyvom na dostupnosť základnej služby,*
- *zneužitie citlivých alebo osobných údajov vo veľkom rozsahu,*
- *incidenty s nadnárodným dopadom vo viacerých štátoch EÚ alebo sveta,*
- *útoky vedené APT skupinami,*
- *incidenty zasahujúce viaceré subjekty naraz,*
- *ransomware útoky.*

Požiadavka na to, aby Expert č. 2 disponoval skúsenosťami s vedením závažných kybernetických bezpečnostných incidentov v pozícii Incident Commander, slúži na zabezpečenie toho, aby osoba zodpovedná za návrh a odborné smerovanie bezpečnostného riešenia mala ***praktickú skúsenosť s reálnymi incidentmi najvyššej závažnosti*** *a rozumela ich priebehu, dopadom a rozhodovacím procesom a tieto vedomosti boli zahrnuté ako v návrhu tak aj implementácii dodávaného diela.*

Spomenuté skúsenosti sú kľúčové najmä pri návrhu architektúry SOC so zreteľom na jej prepojenie s procesnými väzbami CSIRT, návrhu detekčných pravidiel a korelačných mechanizmov pre pokročilé hrozby, rozhodovaní o tom, ktoré udalosti majú byť monitorované, eskalované a akým spôsobom a nastavení priorít z pohľadu kritických aktív a služieb štátu.

Kvalita týchto návrhov zásadne závisí od toho, či expert rozumie ***reálnemu správaniu APT skupín, fázam útoku a bodom, v ktorých je možné útok efektívne detegovať alebo obmedziť jeho dopady****. Tieto aspekty nie je možné plnohodnotne nahradiť len teoretickými znalosťami alebo skúsenosťami s menej závažnými incidentmi.*

Z tohto dôvodu verejný obstarávateľ považuje uvedenú požiadavku za ***primeranú, vecne súvisiacu s predmetom zákazky a nevyhnutnú z pohľadu zabezpečenia odbornej úrovne navrhovaného riešenia****, a to najmä vzhľadom na kritickosť informačných systémov, ktoré majú byť prostredníctvom budovaného SOC chránené.*

Na záver verejný obstarávateľ uvádza, že cieľom uvedenej požiadavky nie je rozšíriť predmet zákazky o činnosti, ktoré v ňom nie sú obsiahnuté, ale ***zabezpečiť, aby návrh a implementácia riešenia vychádzali zo skúseností s reálnymi hrozbami najvyššej závažnosti****, čím sa zvyšuje pravdepodobnosť, že výsledné dielo bude funkčné, odolné a použiteľné v dlhodobom horizonte.*

Odpoveď na otázku č. 4:

Verejný obstarávateľ považuje otázku uchádzača ako vychádzajúcu z užšieho výkladu opisu predmetu zákazky, ktorý zužuje jeho obsah výlučne na formálne pomenované činnosti alebo samostatné typy služieb. Verejný obstarávateľ považuje za potrebné zdôrazniť, že predmet zákazky je koncipovaný ako ***ucelený odborný celok****, ktorého cieľom je návrh a implementácia efektívneho bezpečnostného monitoringu, a nie ako izolovaný súbor výstupov striktne viazaných na jednotlivé odborné disciplíny.*

Požiadavka na odbornú prax v oblasti threat intelligence preto reflektuje potrebu hlbokého porozumenia aktuálnym hrozbám pre prostredie do ktorého bude dodávané dielo implementované, ako aj technikám a postupom útočníkov smerovaným na takýto typ prostredia. Tieto znalosti sú nevyhnutné na kvalifikované vyhodnotenie výsledkov analýzy prístupových infraštruktúr, správnu identifikáciu možných spôsobov útokov vychádzajúcich z poznatkov získaných z threat intelligence a návrh relevantných detekčných scenárov.

Ako je uvedené v Prílohe č. 1 opisu predmetu zákazky, verejný obstarávateľ požaduje návrh bezpečnostného monitoringu vychádzajúci z výsledkov analýzy prístupových infraštruktúr, identifikácie možných spôsobov útokov a tvorby detekčných pravidiel prostredníctvom use cases mapovaných na MITRE ATT&CK Framework. Práve odborné skúsenosti nadobudnuté v oblasti threat intelligence umožňujú expertom správne prepájať tieto vstupy s reálnymi hrozbami, vyhodnocovať ich relevanciu pre konkrétne prostredie a navrhovať detekčné mechanizmy, ktoré sú v praxi účinné a udržateľné.

Činnosti požadované v rámci projektu si ***nevyhnutne vyžadujú schopnosť pracovať s poznatkami o reálnom správaní hrozieb, ich taktikách, technikách a postupoch (TTPs)****, ktoré sú typicky získavané práve v rámci threat intelligence činností. Skúsenosti z oblasti threat intelligence sú preto kľúčové najmä pri:*

- *výbere relevantných techník a taktík z MITRE ATT&CK Framework, ktoré zodpovedajú konkrétnej*
- *prístupovej infraštruktúre,*
- *rozhodovaní, ktoré ATT&CK techniky sú v danom kontexte realisticky zneužiteľné a majú byť zahrnuté do návrhu use cases,*
- *mapovaní zistených zraniteľností a exponovaných služieb na konkrétne scenáre útokov,*
- *a vyhodnocovaní výsledkov analýz attack surface z pohľadu aktuálnych hrozieb naviazaných na dané prostredie.*

Verejný obstarávateľ zároveň zdôrazňuje, že návrh use cases nemá mať formálny alebo teoretický charakter, ale má vychádzať z ***praktických skúseností s hrozbami, ktoré sa vyskytujú v reálnych incidentoch****, a z poznania toho, akým spôsobom sú tieto hrozby implementované a detegované v prevádzkových SOC prostrediach. Práve tieto znalosti sú typickým výstupom dlhodobej praxe v oblasti threat intelligence, vrátane práce s MITRE ATT&CK Framework v kontexte reálnych incidentov a hrozieb.*

Skúsenosti z threat intelligence sú v kontexte predmetu zákazky relevantné aj pri:

- *zhodnotení, ktoré výsledky analýz prístupových infraštruktúr predstavujú iba teoretické slabiny a ktoré predstavujú reálne riziká,*
- *návrhu priorít medzi jednotlivými use cases,*
- *a návrhu detekčných pravidiel tak, aby reflektovali aktuálne a pravdepodobné hrozby, nie iba všeobecné bezpečnostné scenáre.*

Požiadavka na minimálne 5-ročnú prax v oblasti threat intelligence je preto verejným obstarávateľom považovaná ako ***primeraná, vecne súvisiaca s predmetom zákazky a odôvodnená potrebou zabezpečiť odbornú kvalitu návrhu bezpečnostného monitoringu****, najmä s ohľadom na kritickosť informačných systémov, ktoré sú predmetom ochrany, a ich začlenenie do prevádzky SOC ako súčasti CSIRT MF SR.*

Na záver verejný obstarávateľ opakuje, že cieľom uvedenej požiadavky je ***zabezpečenie toho, aby návrh use cases, detekčných pravidiel a bezpečnostnej architektúry vychádzal zo znalosti reálnych hrozieb vplývajúcich na analyzované ako aj budované prostredie****, čím sa zvyšuje praktická použiteľnosť, efektívnosť a dlhodobá udržateľnosť dodaného riešenia.*

Odpoveď na otázku č. 5:

Verejný obstarávateľ považuje za potrebné uviesť, že otázka uchádzača vychádza z nesprávneho výkladu podmienok účasti uvedených v Prílohe č. 6 – Podmienky účasti a z predpokladu, že všetky vymenované odborné skúsenosti a certifikácie musia byť splnené jednou fyzickou osobou, čo však nie je požiadavkou verejného obstarávateľa.

Ako je výslovne uvedené v Prílohe č. 6 – Podmienky účasti, verejný obstarávateľ umožňuje preukázanie splnenia požiadaviek na Experta č. 2 prostredníctvom najviac dvoch fyzických osôb. Zároveň verejný obstarávateľ považuje za dôležité uviesť, že jednotlivé odborné oblasti uvedené pri Expertovi č. 2 (incident response, digitálna forenzná analýza, threat intelligence, penetračné testovanie a riadenie závažných kybernetických bezpečnostných incidentov) netvoria v praxi izolované disciplíny, ale predstavujú ***vzájomne previazané fázy životného cyklu kybernetického útoku a jeho riešenia****.*

*Tento **vzájomne prepojený súbor odborných disciplín v oblasti kybernetickej bezpečnosti**, ktorého účelom je zabezpečiť schopnosť organizácie **predchádzať kybernetickým hrozbám, včas ich detegovať, kvalifikovane analyzovať a efektívne zvládať kybernetické bezpečnostné incidenty**, predstavuje nevyhnutný odborný základ pre návrh, implementáciu a dodanie diela v požadovanej kvalite. Takto navrhnuté dielo má tvoriť **kľúčovú infraštruktúrnu a procesnú oporu pre preventívne aj reaktívne činnosti vykonávané oddelením CSIRT MF SR**.*

***V prípade absencie uvedených odborných znalostí a praktických skúseností existuje vysoké riziko, že dodané riešenie nebude funkčne a koncepčne spôsobilé plnohodnotne podporovať prevádzkové potreby CSIRT MF SR**, najmä pri riešení reálnych bezpečnostných incidentov a pri reakcii na sofistikované kybernetické útoky. Verejný obstarávateľ preto považuje za nevyhnutné, aby odborný tím disponoval znalosťami a skúsenosťami v uvedených oblastiach už vo fáze návrhu a implementácie riešenia.*

*Stanovením týchto požiadaviek verejný obstarávateľ sleduje legitímny cieľ **minimalizácie rizika dodatočných zásahov do architektúry riešenia**, ako sú následné rekonfigurácie, úpravy alebo prestavby dodaného diela, ktoré by mohli vzniknúť v dôsledku nedostatočne odborne spracovaného návrhu, a ktoré by inak neboli nevyhnutné pri zapojení odborne spôsobilého a skúseného realizačného tímu.*

Verejný obstarávateľ nižšie taktiež uvádza prepojenosť jednotlivých odborných disciplín:

1. ***Incident Response** ako integračný prvok predstavuje centrálnu os, v ktorej sa spájajú výstupy všetkých ostatných oblastí. Využíva threat intelligence na pochopenie kontextu hrozby (kto, prečo, akým spôsobom útočí). Poznatky z oblasti penetračného testovania na identifikáciu realistických vektorov útoku. Forenznú analýzu na technickú analýzu incidentu a potvrdenie jeho rozsahu. Bez znalostí týchto oblastí je incident response redukovaný na formálne kroky bez reálnej efektivity.*
2. ***Forenzná analýza** ako zdroj technickej pravdy analyzuje a poskytuje faktické technické dôkazy, ktoré potvrdzujú alebo vyvracajú hypotézy kladené pri incident response, identifikuje kompromitované systémy, účty a dáta, umožňuje rekonštruovať časovú os útoku. Forenzné poznatky sú vstupom pre incident response rozhodovanie, zdrojom nových detekčných pravidiel v SOC a základom pre spätné obohatenie threat intelligence databáz.*
3. ***Threat Intelligence** ako kontext a predikcia prepája technické zistenia s globálnym kontextom hrozieb. Mapuje taktiky, techniky a procedúry útočníkov tzv. TTP v rámci MITRE ATT&CK. Umožňuje rozlišovať medzi náhodnými a cielenými útokmi. Pomáha identifikovať APT aktérov a ich motiváciu. Bez threat intelligence nie je možné správne priorizovať incidenty, navrhovať relevantné detekčné use cases a efektívne riadiť APT incidenty. Skúsenosti z tejto oblasti sú nesmierne dôležité pri posudzovaní a analyzovaní prístupových infraštruktúr, pretože pomôžu vyberať detekčné pravidlá na základe určenia profilu možných útočníkov a ich používaných taktík, techník a procedúr.*
4. ***Penetračné testovanie** ako znalostný základ útoku poskytuje praktické porozumenie spôsobom kompromitácie systémov a poskytuje ostatným uvedeným disciplínam schopnosť efektívne zamerať sa na rýchle riešenie incidentov. Simuluje reálne techniky útočníkov, odhaľuje slabiny v architektúre a konfigurácii, overuje efektivitu detekčných mechanizmov. Skúsenosti z penetračného testovania sú kľúčové pri návrhu SOC detekčných pravidiel, hodnotení attack surface, posudzovaní reálnej závažnosti zraniteľností.*
5. ***Riadenie incidentov** ako nadstavba všetkých oblastí predstavuje strategickú nadstavbu, ktorá integruje incident response, forenznú analýzu, threat intelligence a penetračné testovanie do jedného riadeného procesu. Vyžaduje schopnosť robiť rýchle rozhodnutia s vysokým dopadom, koordinuje technické, procesné a manažérske aspekty incidentu. Bez pochopenia a reálnych skúseností nie je možné dostatočne efektívne spojiť vedomosti z jednotlivých oblastí tak, aby sa dosiahol požadovaný efekt vplývajúci na návrh funkčného diela, ktorého úlohou je byť dôveryhodnou oporou tímu CSIRT MFSR.*

V zmysle uvedeného verejný obstarávateľ považuje za opodstatnené, aby odborný tím disponoval skúsenosťami a znalosťami naprieč uvedenými oblasťami, keďže kvalita návrhu a realizácie SOC je priamo závislá od schopnosti prepájať tieto disciplíny do jedného funkčného celku.

Verejný obstarávateľ zároveň opätovne zdôrazňuje, že podmienky účasti nevyžadujú kumuláciu všetkých uvedených skúseností a certifikácií v jednej fyzickej osobe, ale umožňujú ich preukázanie prostredníctvom dvoch osôb v rámci expertného tímu. Požiadavky sú preto nastavené primerane, reflektujú reálnu prax v oblasti kybernetickej bezpečnosti a sledujú legitímny cieľ zabezpečenia odbornej kvality dodávaného diela.

Odpoveď na otázku č. 6:

*Verejný obstarávateľ považuje za potrebné opakovane uviesť, že predmet zákazky nemožno zúžiť výlučne na súbor izolovaných technických činností uvedených v skrátenej forme v otázke uchádzača. Predmet zákazky predstavuje **ucelené, komplexné dielo**, ktorého cieľom je návrh, implementácia a integrácia infraštruktúry SOC ako súčasti CSIRT MFSR, schopnej dlhodobo a spoľahlivo zabezpečovať ochranu informačných systémov podporujúcich kritické procesy štátu.*

*Aj keď jednotlivé aktivity zahŕňajú implementáciu hardvéru a softvéru, konfiguráciu technológií, analýzu aktív, identifikáciu attack surface a návrh detekčných pravidiel, ich výsledkom má byť **funkčný a odolný bezpečnostný ekosystém**, ktorý musí správne fungovať aj v krízových situáciách, vrátane scenárov úspešne vedených kybernetických útokov. **Návrh takéhoto riešenia si nevyžaduje iba znalosť konfigurácie technológií, ale predovšetkým schopnosť pochopiť správanie útočníkov, reálne dopady bezpečnostných incidentov a praktické dôsledky architektonických a konfiguračných rozhodnutí v prevádzke.***

***Z tohto dôvodu verejný obstarávateľ pri stanovovaní podmienok účasti postupoval s náležitou odbornou starostlivosťou a vychádzal z predpokladu, že kvalita dodaného diela je priamo podmienená praktickými skúsenosťami expertov s riešením reálnych bezpečnostných incidentov.** Požadované certifikácie a odborná prax v oblastiach ako incident response, digitálna forenzná analýza, threat intelligence alebo penetračné testovanie nie sú samoúčelnými požiadavkami ale slúžia ako **objektívne preukázateľný indikátor odborných schopností** nevyhnutných na návrh účinných detekčných mechanizmov, správne vyhodnotenie attack surface a nastavenie bezpečnostného monitoringu tak, aby bol použiteľný a efektívny aj v prípade závažných incidentov.*

*Verejný obstarávateľ zároveň zdôrazňuje, že opis predmetu zákazky je spracovaný v rozsahu, ktorý detailne definuje cieľový stav infraštruktúry SOC, jej architektúru, požadované bezpečnostné princípy a funkčné väzby medzi jednotlivými komponentmi. Podmienky účasti uvedené v Prílohe č. 6 súťažných podkladov **neduplikujú ani nerozširujú predmet zákazky**, ale ho primerane dopĺňajú z pohľadu požadovanej odbornej úrovne osôb, ktoré budú návrh a realizáciu diela zabezpečovať.*

Z hľadiska dodržania § 10 zákona o verejnom obstarávaní verejný obstarávateľ zabezpečil, aby podmienky účasti neboli diskriminačné ani neprimerane obmedzujúce hospodársku súťaž, a to najmä tým, že:

- *umožnil preukázanie požadovaných znalostí a skúseností prostredníctvom viacerých fyzických osôb v rámci expertného tímu,*
- *akceptuje ekvivalentné certifikácie a porovnateľnú odbornú prax,*
- *a vyhlásil verejné obstarávanie v Úradnom vestníku Európskej únie, čím zabezpečil možnosť účasti hospodárskych subjektov z celého vnútorného trhu Európskej únie.*

Verejný obstarávateľ je preto presvedčený, že stanovené podmienky účasti sú v súlade s § 34 ods. 3 zákona o verejnom obstarávaní, keďže sú vecne, časovo aj odborne prepojené s predmetom zákazky, zodpovedajú jeho rozsahu a kritickosti a sledujú legitímny cieľ zabezpečenia kvality a funkčnosti dodaného diela.

Odpoveď na otázku č. 7:

Verejný obstarávateľ po dôkladnom posúdení otázky a po internej odbornej revízii podmienok účasti uvádza, že neplánuje znižovať ani zmierňovať odborné požiadavky kladené na expertov z hľadiska ich vecného obsahu a odbornej náročnosti, avšak pristúpil k ich vecnému a organizačnému spresneniu.

Na základe tohto prehodnotenia verejný obstarávateľ vyčlenil časť požiadaviek pôvodne zahrnutých v rámci Experta č. 1 (požiadavka d) Experta č. 1) do samostatnej expertnej pozície – Expert č. 4 pre projektový manažment. *Zároveň bola k Expertovi č. 4 doplnená požiadavka na odbornú prax. Konkrétna úprava je uvedená v texte nižšie a bola vykonaná s cieľom jasnejšie oddeliť odborné technické kompetencie od kompetencií riadenia projektu, a tým zvýšiť prehľadnosť, transparentnosť a vecnú primeranosť štruktúry expertného tímu.*

Verejný obstarávateľ zdôrazňuje, že táto úprava nepredstavuje zmenu v rozsahu, charaktere ani odbornej náročnosti predmetu zákazky, ani priznanie neprimeranosti pôvodne stanovených požiadaviek. Ide o spresnenie rozdelenia zodpovedností v rámci expertného tímu, ktoré reflektuje komplexnosť predmetu zákazky a potrebu samostatného riadenia projektu popri odbornom návrhu a implementácii bezpečnostného riešenia.

Verejný obstarávateľ má za to, že rozsah a charakter podmienok účasti bol v predchádzajúcich odpovediach na jednotlivé otázky v rámci tejto žiadosti o vysvetlenie opakovane podrobne, vecne a dostatočne odôvodnený. Zároveň bolo vysvetlené, že predmet zákazky nemožno posudzovať len ako súbor izolovaných technických činností definovaných v Prílohe č. 1 a č. 10, ale ako ucelené dielo, ktorého výsledkom má byť funkčný, stabilný a bezpečný systém SOC, schopný plniť svoju úlohu aj v prípade krízových a mimoriadnych bezpečnostných situácií.

Verejný obstarávateľ naďalej zdôrazňuje, že podmienky účasti nie sú stanovené samoúčelne ani s cieľom obmedziť hospodársku súťaž, ale slúžia na zabezpečenie primeranej odbornej úrovne osôb, ktoré budú zodpovedné za návrh, koordináciu a realizáciu diela. Ako bolo uvedené v predchádzajúcich odpovediach, požadované certifikácie a odborná prax predstavujú požiadavku na objektívny a overiteľný indikátor schopnosti expertov navrhnúť riešenie, ktoré bude v praxi použiteľné, odolné, udržateľné a schopné podporovať činnosť CSIRT MFSR.

Verejný obstarávateľ zároveň opakovane poukazuje na skutočnosť, že:

- *podmienky účasti umožňujú preukázanie požadovaných znalostí a skúseností prostredníctvom viacerých fyzických osôb v rámci expertného tímu,*
- *akceptujú sa ekvivalentné certifikácie a porovnateľná odborná prax,*
- *a vyhlásil verejné obstarávanie v Úradnom vestníku Európskej únie, čím zabezpečil možnosť účasti hospodárskych subjektov z celého vnútorného trhu Európskej únie.*

Na základe uvedeného má verejný obstarávateľ za to, že aj po vykonanom spresnení sú stanovené podmienky účasti primerané predmetu zákazky, v súlade s § 34 ods. 3 zákona o verejnom obstarávaní a neporušujú zásadu hospodárskej súťaže podľa § 10 zákona. Verejný obstarávateľ preto nepovažuje za dôvodné pristúpiť k ďalším úpravám podmienok účasti.

Na základe vyššie uvedeného verejný obstarávateľ:

1. <u>upravuje</u> znenie Minimálnej požadovanej úrovne štandardov v bode 2.3.3 Prílohy č. 6 súťažných podkladov „Podmienky účasti" pri Expertovi č.1 nasledovne:

<u>Expert č. 1 - IT bezpečnostný architekt/audítor:</u>

Uchádzač môže použiť na preukázanie splnenia nižšie uvedených podmienok účasti na pozíciu Experta č. 1 maximálne 2 fyzické osoby*.*

a) ***Platný certifikát CISSP*** *alebo* ***CASP+*** *získaný úspešným absolvovaním certifikačnej skúšky od akreditovaných organizácií alebo združení, ako sú napríklad* ***SANS****,* ***EC-Council****,* ***GIAC****,* ***ISC²****,* ***Offensive Security****,* ***eLearnSecurity****,* ***CompTIA*** *alebo ekvivalentný certifikát od inej uznávanej autority.* ***Certifikáty vydané len na základe absolvovania školenia bez skúšky nie sú akceptované.***
Podmienku účasti uchádzač preukáže prostredníctvom kópie certifikátu.

b) ***Minimálne 5 - ročná odborná prax ako IT bezpečnostný architekt*** *s návrhom a posudzovaním* ***high-level/low-level design*** *riešeniami v oblasti enterprise architektúry, bezpečnostného softvéru a aplikácií, optimalizácie softvérových riešení alebo integrácií.*
Podmienku účasti uchádzač preukáže štruktúrovaným profesijným životopisom alebo ekvivalentným dokladom.

c) *Znalosť tvorby a udržiavania architektonickej dokumentácie a ovládanie štandardov:* ***ArchiMate alebo UML alebo TOGAF 9 alebo BPMN alebo ekvivalent****;*
Podmienku účasti uchádzač preukáže prostredníctvom kópie aspoň jedného z certifikátov.

~~d) ***Platný certifikát PRINCE 2*** *alebo* ***SCRUM*** *alebo* ***SAFE*** *alebo* ***PM²*** *na odbornú spôsobilosť pre riadenie projektov alebo ekvivalent daného certifikátu od inej akreditovanej autority;*
Podmienku účasti uchádzač preukáže prostredníctvom kópie certifikátu.~~

d) ***Minimálne 3 preukázateľné pracovné skúsenosti*** *s implementáciou bezpečnostných politík a štandardov v oblasti kybernetickej bezpečnosti, ako sú* ***ISO/IEC 27001, NIST, ENS*** *alebo ekvivalent;*
Podmienku účasti uchádzač preukáže štruktúrovaným profesijným životopisom alebo ekvivalentným dokladom.

e) ***Minimálne 3 - ročná odborná prax*** *v oblasti analýzy rizík kybernetickej bezpečnosti vrátane identifikácie hrozieb, hodnotenia zraniteľností a návrhu opatrení na zmiernenie rizík;*
Podmienku účasti uchádzač preukáže štruktúrovaným profesijným životopisom alebo ekvivalentným dokladom.

2. ***dopĺňa znenie Minimálnej požadovanej úrovne štandardov v bode 2.3.3 Prílohy č. 6 súťažných podkladov „Podmienky účasti“ o Experta č.4 – Projektový manažér nasledovne:***

Expert 4 – Projektový manažér

Uchádzač preukáže splnenie nižšie uvedených podmienok účasti na pozíciu Experta č. 4 maximálne 1 fyzickú osobu.

a) ***Minimálne 3 - ročná odborná prax*** *v oblasti projektového riadenia.*
Podmienku účasti uchádzač preukáže štruktúrovaným profesijným životopisom alebo ekvivalentným dokladom*.*

b) ***Platný certifikát PRINCE 2*** *alebo* ***SCRUM*** *alebo* ***SAFE*** *alebo* ***PM²*** *na odbornú spôsobilosť pre riadenie projektov alebo ekvivalent daného certifikátu od inej akreditovanej autority;*
Podmienku účasti uchádzač preukáže prostredníctvom kópie certifikátu.

Záver

Na základe vyššie uvedených špecifík verejný obstarávateľ považuje za **odôvodnené a primerané**, aby na realizáciu predmetu zákazky boli kladené **vyššie nároky na odborné znalosti a skúsenosti kľúčových expertov**, než je bežné v menej kritických sektoroch.

Prísnejšie znalostné štandardy sú opodstatnené najmä tým, že experti sa podieľajú na návrhu riešenia, ktoré **priamo podporuje ochranu finančnej stability štátu**, riešenie musí byť schopné **detegovať a správne vyhodnocovať incidenty s potenciálne okamžitým finančným dopadom**, architektúra SOC musí zohľadňovať **vysoké nároky na dostupnosť, integritu a rýchlosť reakcie** a odborné rozhodnutia prijímané v priebehu návrhu a implementácie majú **dlhodobý vplyv na bezpečnostnú odolnosť kritických systémov**.

Verejný obstarávateľ preto vyžaduje expertov, ktorí majú **preukázateľné skúsenosti v požadovaných oblastiach**, rozumejú riadeniu bezpečnostných incidentov a sú schopní navrhovať bezpečnostné riešenia s ohľadom na systémové riziká.

Požiadavky obsiahnuté v podmienkach účasti taktiež priamo reflektujú povinnosti Zhotoviteľa vyplývajúce zo zmluvného rámca, najmä zo **„ZMLUVY O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ A**

NOTIFIKAČNÝCH POVINNOSTÍ“, ktorá je súčasťou súťažných podkladov p*ríloha č. 2 – Zmluva*, a ktorá kladie dôraz na:

- plnenie bezpečnostných opatrení podľa zákona o kybernetickej bezpečnosti,
- schopnosť správne identifikovať, vyhodnotiť a eskalovať bezpečnostné udalosti a kybernetické bezpečnostné incidenty,
- zabezpečenie súladu s notifikačnými povinnosťami voči príslušným orgánom.

Z uvedeného dôvodu verejný obstarávateľ považuje za nevyhnutné, aby osoby podieľajúce sa na návrhu a implementácii riešenia mali **reálne skúsenosti s tým, ako sa navrhované architektúry, detekčné mechanizmy a procesy správajú v krízových situáciách ako aj v rámci závažných kybernetických bezpečnostných incidentov**.

Verejný obstarávateľ je presvedčený, že podmienky účasti a znalostné štandardy expertov predstavujú **primeranú reakciu na charakter a význam predmetu zákazky** sledujúci legitímny cieľ ochrany kľúčových záujmov štátu, sú v súlade s princípmi zákona o verejnom obstarávaní **a princípmi rovnakého zaobchádzania a nediskriminácie**. Zároveň vytvárajú predpoklady na to, aby výsledkom verejného obstarávania bolo funkčné a dlhodobo udržateľné riešenie SOC, schopné riadne plniť svoje úlohy v rámci CSIRT MF SR bez potreby dodatočnej realizácie nápravných opatrení vyplývajúcich z nedostatočnej znalosti procesov CSIRT zo strany dodávateľa.

Zároveň Vám týmto oznamujeme, že na základe vyššie uvedenej doručenej žiadosti o vysvetlenie informácií potrebných na vypracovanie ponuky verejný obstarávateľ:

a) **v súvislosti s odpoveďou na otázku č. 7 zverejní aktualizovanú Prílohu č. 6 súťažných podkladov „Podmienky účasti“ v systéme JOSEPHINE.**

b) **predlžuje lehotu** na predkladanie ponúk a lehotu na otváranie ponúk nasledovne:
Lehota na predkladanie ponúk: 19. 1. 2026 o 9.00 hod.
Lehota na otváranie ponúk: 19. 1. 2026 o 10.00 hod.

c) uvedené zmeny lehôt budú publikované v Úradnom vestníku EÚ a vo Vestníku verejného obstarávania v rámci redakčnej opravy.

S pozdravom

Ing. Dáša Lauková
generálna riaditeľka sekcie verejného obstarávania