Číslo spisu: NBS1-000-071-638

Záznam číslo: 100-000-353-292

ZÁPISNICA Z PRÍPRAVNÝCH TRHOVÝCH KONZULTÁCIÍ

Názov verejného obstarávateľa:	Národná banka Slovenska
Sídlo verejného obstarávateľa:	Imricha Karvaša 1, 813 25 Bratislava
Názov účastníka:	Atos IT Solutions and Services s.r.o.
Adresa účastníka:	Pribinova 19, 811 09 Bratislava, Slovensko
Predmet / názov PTK:	SIEM SOC (Security Operation Center)
Postup:	Prípravné trhové konzultácie (ďalej len „PTK“)
Legislatívny rámec:	Podľa § 25 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)
Dokumenty a bližšie informácie k PTK:	https://nbs.sk/o-narodnej-banke/verejne-obstaravanie/ptk/ https://www.nbs.sk/sk/verejne-obstaravanie/ptk
Lehota na prihlásenie k účasti na PTK:	6.5.2022, do 14:00 h
Miesto uskutočnenia PTK:	Národná banka Slovenska, Imricha Karvaša 1, 813 25 Bratislava
Dátum a čas uskutočnenia PTK:	17.05.2022, 09:30 h

Pred začatím oficiálneho postupu verejného obstarávania realizuje Národná banka Slovenska v súlade s § 25 zákona o verejnom obstarávaní prípravné trhové konzultácie. Cieľom PTK je spresnenie technických požiadaviek na služby SOC a získanie informácií týkajúcich sa obchodných podmienok dodania služby. Tieto informácie poslúžia ako podklad pre prípravu súťažných podkladov plánovaného verejného obstarávania služieb SIEM Security Operation Center (SOC).

PTK predchádzalo dňa 26.04.2022 zverejnenie Výzvy na účasť na PTK (ďalej len „výzva") s prílohami na webovom sídle NBS na adrese: https://nbs.sk/o-narodnej-banke/verejne-obstaravanie/ptk/. Zverejnením Výzvy bolo zároveň umožnené, aby sa týchto konzultácií mohlo zúčastniť široké spektrum hospodárskych subjektov, prípadne tretieho sektora.

Prípravných trhových konzultácií sa za Národnú banku Slovenska zúčastnili:

Ivan Cibiri, vedúci oddelenia informačnej bezpečnosti

Martin Stanek, expert informačnej bezpečnosti

Peter Červený, expert informačnej bezpečnosti

Ján Debnár, expert kybernetickej bezpečnosti

Prípravných trhových konzultácií sa za firmu ATOS IT Solutions and Services s.r.o. zúčastnili:

Benjamín Würfl

Michal Sekula

Milan Paštrnák

Na úvod PTK p. Ivan Cibiri privítal prítomných účastníkov a podal bližšie informácie o plánovanom priebehu a cieľoch PTK. Takisto účastníkov PTK oboznámil o vyhotovení audio záznamu z PTK pre účely vyhotovenia zápisnice z priebehu PTK, ktorý bude po jej verifikácii následne zlikvidovaný.

Nasledovala diskusia k nasledovným bodom podľa prílohy 4 – Úvodné témy na diskusiu SIEM SOC.

1. Predmet zákazky

a) Sú zrozumiteľné všetky požiadavky NBS
b) Sú technické požiadavky NBS dostatočne definované, resp. čo je potrebné spresniť aby bolo možné vypracovať záväznú ponuku vo verejnom obstarávaní

Diskusia k bodu:

- Zo strany NBS bol vznesená požiadavka na finančne efektívne riešenie SIEM SOC.
- Účastník navrhuje SIEM SOC postaviť na produktoch ktoré má vo svojom portfóliu. V tejto súvislosti podotkol, že pri výbere produktu je potrebné prihliadať nielen na cenu ale aj na jeho rozšírenosť.
- Účastník odporúča v rámci technických požiadaviek na SOC doplniť parameter objem spracovávaných dát v GB/deň kvôli licencovaniu produktov a túto informáciu mu poslať na spresnenie odhadu nákladov.
- Účastník oboznámil NBS, že všetky produkty v jeho portfóliu sú poskytované formou subscription a to buď on-premise alebo ako cloudové riešenie. Náklady na on-premise riešenie závisia, či bude prevádzkované vo virtuálnom prostredí NBS alebo na dedikovanom HW a prípadne v HA režime. Účastník odporúča, aby tieto technicko-obchodné informácie boli zadefinované v požiadavkách na SOC.

- Účastník potvrdil, že všetky požiadavky NBS mu boli zrozumiteľné.

2. Technické požiadavky

Diskusia k bodu:

- Účastník a NBS si vzájomne vyjasnili technické prístupy a odlišnosti jednotlivých produktov k zberu informácií zo zdrojov formou agentov.

3. Podmienky súťaže

a) Aké máte úspešné referencie na SOC za posledné 2 roky (bankový sektor?)
b) Aké je zloženie SOC tímu (odborná kvalifikácia a skúsenosti v projektoch)
c) Ako sa dajú overiť skúsenosti a odborná pripravenosť SOC tímu
d) Koľko času potrebujete na prípravu ponuky

Diskusia k bodu:

- Účastník spresnil a doplnil informácie k svojím referenciám uvedeným v dotazníku.
- Účastník spresnil a doplnil informácie k SOC tímu uvedenému v dotazníku.
- Účastník objasnil rozsah a obsah ním poskytovaných služieb v rámci SOC.
- Účastník objasnil možnosti poskytovania SOC služieb v rôznych jazykoch (SK, CZ, EN) na území EÚ.
- Účastník odporúča spresniť v prílohe 3 – Špecifikácia služieb a aktivít SIEM SOC (PTK) pre službu „Monitoring bezpečnosti IT" časové pokrytie podieľania interného SOC teamu na riešení bezpečnostných incidentov.
- Účastník spresnil a doplnil informácie k času potrebnému na prípravu ponuky.
- Aby sa predišlo nedorozumeniam v terminológii, účastník navrhuje upresniť pojmy „SIEM" a „SOC" používané v diskutovanej dokumentácií NBS (SIEM ako skupina riešení LogRhythm + Netmon + Flowmon).
    - SIEM (Security Incident and Event Management) je centralizovaný informačný panel bezpečnostných informácií používaný na monitorovanie prevádzky a bezpečnosti siete a komponentov IT, na analýzu, korelovanie a na zobrazovanie upozornení o podozrivých aktivitách v sieti. V prostredí NBS je to aktuálne LogRhythm.
    - SOC (Security Operations Center) je zvyčajne fyzická miestnosť v organizácii, kde niekoľko zamestnancov nepretržite monitoruje sieťovú prevádzku, výstrahy a vizualizované informácie, na základe ktorých reaguje na potenciálny kybernetický incident. SOC sa zameriava skôr na bezpečnosť siete než na jej výkon a využitie.

      SOC a SIEM sú rôzne stratégie, ktoré spolupracujú a dopĺňajú sa pri odhaľovaní a riešení kybernetické udalosti. SIEM musí byť nakonfigurovaný tak, aby do SOC posielal správne upozornenia a podrobné informácie, aby SOC tím na základe zistenej hrozby mohol rýchlo určiť správne kroky.

      Flowmon je samostatný produkt na monitoring sieťovej prevádzky a môže slúžiť ako zdroj logov pre SIEM.

4. Obchodné podmienky

a) Aké sú možnosti škálovateľnosti služby (zvyšovanie/znižovanie počtu monitorovaných zariadení, zmena počtu udalostí za jednotku času a pod.)
b) Aké sú podmienky odovzdania know-how po skončení zmluvy
c) Aké sú podmienky pri predčasnom ukončení zmluvného vzťahu: platnosť licencií, transfer know-how, ...

Diskusia k bodu:

- Účastník spresnil a doplnil informácie k možnostiam škálovateľnosti služby formou subscription na ročnej báze a platieb vopred na celé obdobie.
- Účastník spresnil a doplnil informácie k odhadu nákladov a spôsobu riešenia dočasného prekročenia licencií.
- Účastník spresnil a doplnil informácie k podmienkam odovzdania know-how a dĺžke trvania štandardnej výpovednej lehoty ako aj podmienky pri predčasnom ukončení zmluvného vzťahu.
- Účastník odporúča do požiadaviek na cloudové riešenie SOC doplniť požiadavku na prístup do archívu SOC po skončení poskytovania služieb SIEM SOC. Dáta patria zákazníkovi, má právo si urobiť backup na lokálne médiá. Keďže SIEM zhromažďuje logy z rôznych zdrojov a informácie agreguje na jednom mieste, logy musia byť uložené lokálne, alebo v cloude a to vyžaduje dostatok úložného priestoru. Tento úložný priestor je potrebné odhadnúť, ideálne formou PoC (Proof of Concept).

5. Dodacie podmienky

a) Aké sú nároky na technické vybavenie, procesy NBS, počet a odbornú spôsobilosť personálu NBS (napr. zaškolenie)
b) Aká je odhadovaná doba na prípravu spustenia služby od podpisu zmluvy

Diskusia k bodu:

- Účastník spresnil a doplnil informácie k odhadovanej dobe nasadenia nového SIEMu.
- Riešenia môžu byť implementované vo forme hardvérových appliances, alebo ako virtuálne appliances na virtuálnej platforme zákazníka (VMWare, HyperV atď.). Každý vendor má uvedené svoje špecifické požiadavky na technické vybavenie a tie závisia od konkrétneho návrhu riešenia.

6. Rôzne

V bode Rôzne bol ponechaný priestor na otázky účastníkov PTK.

Diskusia k bodu:

Na záver PTK bola zopakovaná informácia, že sa od účastníka PTK očakáva verifikácia zápisnice v lehote do 24.05.2022. A takisto, že po ukončení PTK verejný obstarávateľ zverejní zápisnice z priebehov PTK na svojom webovom sídle na adrese https://nbs.sk/o-narodnej-banke/verejne-obstaravanie/ptk/.