Číslo spisu: NBS1-000-071-638

Záznam číslo: 100-000-353-295

ZÁPISNICA Z PRÍPRAVNÝCH TRHOVÝCH KONZULTÁCIÍ

Názov verejného obstarávateľa:	Národná banka Slovenska
Sídlo verejného obstarávateľa:	Imricha Karvaša 1, 813 25 Bratislava
Názov účastníka:	SOITRON s.r.o.
Adresa účastníka:	Plynárenská 5, 829 75 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:	31.05.2022, 9:00 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 SOITRON s.r.o. zúčastnili:

Bruno Veselý

Martin Lohnert

Stanislav Smolár

Michal Šimkovič

Maroš Rajnoch

Ján Benka

Marek Madžo

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:

- Účastník potvrdil, že všetky požiadavky NBS mu boli zrozumiteľné.
- Účastník navrhuje spresniť aktivity „Úvodné prešetrenie podozrivých zistení" a „Detailné prešetrenie bezpečnostných incidentov" v zmysle ich využitia.
- Účastník navrhuje spresniť štruktúru a minimálny rozsah evidovaných informácii v denníku bezpečnostných zistení SIEM.
- NBS objasnila účel použitia prevádzkového denníka SIEM v zmysle evidencie vykonaných zmien v SIEMe.

- Účastník navrhuje spresniť požiadavku na „opatrenia na zamedzenie opakovania incidentov".
- NBS objasnila formuláciu „Podieľať sa na riešení" v zmysle, že externý SOC bude súčinný pri riešení incidentu až do jeho vyriešenia a mitigácie. Aktívny zásah bude v kompetencii NBS.
- Účastník odporúča spresniť informácie ohľadom komunikačnej matice, resp. kto bude pre externý SOC tím komunikačný partner na strane NBS (interný SOC tím, správcovia, eskalačný kontakt a pod.)
- Účastník informoval NBS o možnosti poskytovať službu aktívneho incident response nad kritickým scenármi, t.j. vopred schválený zásah. Účastník uvedie popis tejto služby do dotazníka.
- NBS vysvetlil poskytnutie vzdialeného prístupu v zmysle, že bude pre každého člena z externého SOC tímu vytvorený samostatný virtuálny desktop s prístupom na SIEM zariadenia. V prípade potreby bude možné dočasne vytvoriť aj on-site pracovisko. NBS nepredpokladá zriadenie trvalého on-site pracoviska.
- Účastník a NBS diskutovali o možnostiach integrácie NBS SIEMu do SOC účastníka.
- Účastník odporúča, aby v špecifikácii bola exaktne popísaná požiadavka na aktívny threat hunting.
- Účastník odporúča, aby bol v špecifikácii jasne vymedzený rozsah a účel aktivity „Vyriešenie vzniknutého problému odhaleného pri monitorovaní SIEMu ..." v zmysle, že sa jedná o riešenie problémov s konfiguráciou SIEMu a nie riešenie problémov s nefunkčnosťou technológie SIEMu.
- Účastník odporúča spresniť účel a zameranie služieb „Rozvoj SIEMu" a „Optimalizácia SIEMu" s cieľom zamedziť prekrývanie aktivít.
- NBS informovala, že nedisponuje automatizačnou platformou (SOAR) na orchestráciu a automatizáciu bezpečnostných operácií, incident response a threat hunting workflow.
- Účastník odporúča spresniť existujúce prostredie/nástroje NBS pre službu „Sledovanie IT hrozieb a zraniteľností".
- Účastník a NBS diskutovali o potrebe aktuálnych informácií v Asset Management-e.
- Účastník navrhuje do špecifikácie doplniť parameter flow za sekundu.
- NBS potvrdila informácie o počte informačných systémov, zdrojov, počte udalostí, atď. uvedených v prílohe 2.
- Účastník odporúča doplniť koľko zistení/bezpečnostných incidentov sa priemerne rieši v súčasnosti.

2. Technické požiadavky

Diskusia k bodu:

- Témy boli rozdiskutované v ostatných bodoch.

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 uvedie v dotazníku informácie o svojich referenciách.
- Účastník uvedie v dotazníku informácie o odbornej spôsobilosti svojich zamestnancov.
- Účastník uvedie v dotazníku možnosti overenia skúseností s poskytovaním služieb SIEM SOC.
- Účastník uviedol počet dní ktoré potrebuje na prípravu ponuky.

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 odhadované náklady pre jednotlivé možnosti služby
c) Aké sú podmienky odovzdania know-how po skončení zmluvy
d) Aké sú podmienky pri predčasnom ukončení zmluvného vzťahu: platnosť licencií, transfer know-how, ...

Diskusia k bodu:

- Účastník uvedie v dotazníku možnosti škálovania poskytovaných služieb.
- Účastník odporúča spresniť požiadavky NBS na odovzdanie know-how.

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 uvedie v dotazníku požiadavky, ktoré je potrebné na strane NBS zabezpečiť na spustenie a fungovanie služby SIEM SOC.
- Účastník uvedie v dotazníku postup a fázy prípravy spustenia služby.

6. Rôzne

V bode Rôzne bol ponechaný priestor na otázky účastníkov PTK.

Diskusia k bodu:

- Účastník informoval NBS o možnostiach poskytovania služieb forenznej analýzy.
- Účastník uvedie v dotazníku odporúčania na kontrolu kvality služby SOC SIEM.

Na záver PTK bola zopakovaná informácia, že sa od účastníka PTK očakáva verifikácia zápisnice a zaslanie odpovedí k otázkam v prílohe č. 5 Dotazník SIEM SOC v lehote do

10.06.2022. 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/.