Číslo spisu: NBS1-000-106-411

Číslo záznamu: 100-000-885-390

Dátum: 15.4.2025

**VYSVETLENIE**

informácií potrebných na vypracovanie ponuky a na preukázanie splnenia podmienok účasti podľa § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“)

Národná banka Slovenska so sídlom Imricha Karvaša 1, 813 25 Bratislava (ďalej len „verejný obstarávateľ“) obdržala prostredníctvom elektronického prostriedku, komunikačného rozhrania systému JOSEPHINE žiadosti o vysvetlenie podľa § 48 ZVO týkajúce sa predmetnej zákazky.

Po podrobnom oboznámení sa so žiadosťami o vysvetlenie Vám verejný obstarávateľ poskytuje nasledujúce vysvetlenie:

**Otázka č.1**

V prílohe 9 SP Opis predmetu zákazky, záložka MBIT (SIEM a NDR) poradové číslo 2.86 píšete „NetFlow analyzátor musí umožniť spracovať v každej lokalite LAN minimálne 5000 flows/s“ a 2.87 píšete “ NDR infraštruktúra musí na každej lokalite umožniť uložiť udalosti po dobu min. 1 roka“.

Podľa vyššie spomínaných podkladov 2.86 a 2.87 je podľa našich skúseností je neobvyklé ukladať udalosti po dobu jedného roka.

Otázka: počíta obstarávateľ, že na 5000 flows/s a ukladanie udalostí počas jedného roka bude potrebný kolektor o veľkosti 48TB na každej lokalite?

Je možné, že obstarávateľ prehodnotí dobu ukladania udalostí na obvyklú dobu (2-3) mesiace a bude potom postačovať kolektor o veľkosti 12 TB na každú lokalitu?

**Odpoveď:**

Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že požiadavky na NDR infraštruktúru, t.j. spracovanie minimálne 5000 flows/s a retencia uložených dát 1 rok vychádzajú z technických špecifikácií súčasných zariadení a neuvažujeme o ich prehodnotení. Tak ako sme uviedli v podkladoch verejného obstarávania, súčasné priemerné vyťaženie NDR je odhadom 1500 flows/s s dobou retencie dát na disku cca 1 rok.

**Otázka č. 2**

V návrhu zmluvy o monitoringu kybernetickej bezpečnosti v článku VIII bod 2 požadujete mať „uzatvorené poistenie všeobecnej zodpovednosti za škodu s minimálnou poistnou sumou vo výške 100.000,- eur (slovom sto tisíc eur). Poistením musia byť kryté nároky všeobecnej zodpovednosti za škodu na veciach a na zdraví, vrátane ušlého zisku, spôsobené pri výkone činností poskytovateľa na základe tejto Zmluvy spôsobenej objednávateľovi alebo tretím osobám, pričom toto poistenie musí mať vinkuláciu v prospech objednávateľa, čiže viazané poistné plnenie v prospech objednávateľa, resp. príkaz vyplatiť poistné plnenie objednávateľovi.“ Otázka: žiadna poisťovacia spoločnosť, ktorú sme oslovili sa nikdy nestretla s podmienkou mať poistenie všeobecnej zodpovednosti za škodu vinkulovanú v prospech Národnej banky Slovenska a to aj z dôvodu, že je to ich regulačný orgán. Bude v takomto prípade postačovať „uzatvorené poistenie všeobecnej zodpovednosti za škodu s minimálnou poistnou sumou vo výške 100.000,- eur (slovom sto tisíc eur). Poistením musia byť kryté nároky všeobecnej zodpovednosti za škodu na veciach a na zdraví, vrátane ušlého zisku, spôsobené pri výkone činností poskytovateľa na základe tejto Zmluvy spôsobenej objednávateľovi alebo tretím osobám“ bez viazanej vinkulácie? Ak nie, vie obstarávateľ vymenovať finančné subjekty (poisťovne) , ktoré takýto produkt na Slovenskom trhu poskytujú?

**Odpoveď:**

Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že nebude požadovať predmetné poistenie s vinkuláciou v prospech verejného obstarávateľa ako budúceho objednávateľa, pričom v zmysle uvedeného upravuje v článku VIII bod 2 návrhu Zmluvy na poskytovanie služieb monitoring kybernetickej bezpečnosti č. C-NBS1-000-106-915 tak, že vypúšťa text: „... *,pričom toto poistenie musí mať vinkuláciu v prospech objednávateľa, čiže viazané poistné plnenie v prospech objednávateľa, resp. príkaz vyplatiť poistné plnenie objednávateľovi*.“ a zároveň za slovo „... osobám“ dopĺňa interpunkčné znamienko bodku. Verejný obstarávateľ štandardne žiada predmetné poistenie bez vinkulácie a v tomto prípade sa jednalo o chybu v písaní.

**Otázka č.3**

V návrhu zmluvy o monitoringu kybernetickej bezpečnosti v článku XI bod 1 požadujete aby sa poskytovateľ mal do 6 mesiacov od účinnosti zmluvy tri vyškolené osoby na jednotlivé certifikáty, postačuje jeden z nich.

Otázka:

Na stránke výrobcu Trellix v sekcii vzdelávanie, nie je možné takéto certifikáty nájsť a teda získať. Vie obstarávateľ (keďže to požaduje) poskytnúť možným poskytovateľom služby informáciu, kde je možné takéto certifikáty získať?

**Odpoveď:**

Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že podľa informácii od výrobcu, Trellix prechádza na platformu Seismic a z toho dôvodu nie sú dostupné niektoré technické kurzy. V súčasnej dobe je dostupný alternatívny certifikačný kurz, a to Technical Specialist Certifications: Trellix Endpoint Security, ktorý je možné získať po prihlásení na Trellix Portál ako partner a následne v portáli v rámci Trellix University získať prístup na Seismic portál, kde nájdete tento kurz. Druhý alternatívny certifikačný kurz je voľne dostupný na <https://training-catalog.trellix.com/Course/148202/exam-endpoint-detection-and-response> ako Exam: Endpoint Dtection and Response, preto bude verejný obstarávateľ akceptovať tiež obidva spomenuté alternatívne certifikačné kurzy.

Na základe vyššie uvedeného verejný obstarávateľ ako budúci objednávateľ pre vylúčenie pochybností dopĺňa text v článku XI bod 1 návrhu Zmluvy na poskytovanie služieb monitoring kybernetickej bezpečnosti č. C-NBS1-000-106-915, tak že dopĺňa výpočet certifikátov o *Technical Specialist Certifications: Trellix Endpoint Security, Exam: Endpoint Detection and Response.*

**Otázka č.4**

V návrhu zmluvy o monitoringu kybernetickej bezpečnosti v článok I, bod 2 sú vymenované služby, ktoré sa poskytovateľ zaväzuje poskytovať. V tých službách nie je spomenutá služba EDR (Endpoint Detection and Response). Je spomenutý len záväzok poskytovateľa používať pri poskytovaní predmetu planenia Trellix EDR.

Otázka:

Keďže celé obstarávanie je koncipované ako poskytovanie služby poskytovateľa služieb bezpečnostného monitoringu, je možné aby poskytovateľ služby mohol poskytnúť rovnako kvalitnú službu EDR (Endpoint Detection and Response) na inej technológii ako je Trellix EDR?

**Odpoveď:**

Verejný obstarávateľ si Vám dovoľuje uviesť, že z dôvodu, že verejný obstarávateľ má nasadené produkty Trellix na všetkých pracovných staniciach, ako aj na väčšine serverov formou agentov, tak nie. Duplicitné riešenie nie je žiadúce.

**Otázka č.5**

V opise predmetu ani sútažných podkladoch nie je spomenuté, či obstarávateľ poskytne virtuálne zdroje pre kolektor na zaistenie zberu logov, alebo bude povinnsoťou poskytovateľa dodať HW zdroje do prostredia objednávateľa.

Otázka:

Poskytne obstarávateľ virtuálne zdroje pre kolektor na zaistenie zberu logov?

**Odpoveď:**

Nie, verejný obstarávateľ ako objednávateľ neposkytne virtuálne zdroje pre kolektor na zaistenie zberu logov. Verejný obstarávateľ si Vám dovoľuje uviesť, že povinnosťou budúceho poskytovateľa je v rámci poskytovaných služieb zabezpečiť si potrebný HW a SW do prostredia verejného obstarávateľa ako objednávateľa.

**Otázka č.6**

Môže obstarávateľ upresniť aké detekčné pravidlá sú dnes nastavené v SIEM riešení mimo špecifických use-case a to v rovnakom detaile ako v Prílohe 7 Zoznam špecifických use-case?

Informácie sú dôležité pre odhad pracnosti migrácie na dodávaný SIEM v rámci služby.

**Odpoveď:**

Verejný obstarávateľ si Vám dovoľuje uviesť, že Zoznam aktuálne používaných detekčných pravidiel v SIEMe prikladá ako prílohu odpovede na Vašu žiadosť o vysvetlenie v priloženom súbore „Detekčné pravidlá v SIEMe.txt“[[1]](#footnote-1).

**Otázka č.7**

V prílohe 9 SP Opis predmetu zákazky, záložka MBIT (SIEM a NDR) poradové číslo 2.96 píšete „spracovať minimálne 5000 (priemer za 24 hodín) záznamov za sekundu (EPS)“. Pre správne nacenenie služby je pre nás relevantné sa zoznámiť s priebehom minimálnych a maximálny EPS v priebehu času.

Otázka:

Môže poskytovateľ sprístupniť štatistiku vývoja EPS za jeden štandardný týždeň alebo jeden kalendárny mesiac?

**Odpoveď:**

Verejný obstarávateľ si Vám dovoľuje uviesť, že nevyhodnocuje štatistiky vývoja EPS. Hodnota EPS kolíše a pohybuje sa odhadom medzi 1000 až 10 000. Samotný SIEM v rámci merania využitia licencií vyhodnocuje EPS ako priemer EPS za 24 hodín. Za posledných 30 dní bola SIEMom nameraná maximálna priemerná hodnota za 24 hodín 2766 EPS.

**Otázka č.8**

V prílohe 9 SP Opis predmetu zákazky, záložka Skenovanie zraniteľnosti poradové číslo 2.153 „Podpora pre integráciu s Password Vault riešeniami – napr. HashiCorp Vault a pod.“

Otázka: Ako si obstarávateľ predstavuje podporu pre intergáciu a k čomu má intergácia slúžiť?

**Odpoveď:**

Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že integrácia má umožniť ukladanie a následné využívanie credentials pre skenovanie centralizovane v takýchto Vault riešeniach. Verejný obstarávateľ požaduje také riešenie, ktoré bude v prípade potreby možné nakonfigurovať tak, aby neukladalo credentials lokálne, ale využilo vhodné Vault riešenie.

**Otázka č.9:**

Prosíme o informáciu, či predmetom verejného obstarávania je aj dodanie nového HW a SW pre službu SIEM a NDR súčasne i implementačná fáza nového SIEM a NDR alebo len zmena poskytovateľa pre službu SIEM a NDR, kde nový poskytovateľ bude využívať aktuálne použitú a nasadenú platformu SIEM a NDR a len ju prevezme od iného poskytovateľa.

**Odpoveď:**

Predmetom zákazky nie je dodanie HW a SW pre verejného obstarávateľa ako budúceho objednávateľa. Povinnosťou budúceho poskytovateľa je v rámci poskytovaných služieb zabezpečiť si všetok potrebný HW a SW do prostredia verejného obstarávateľa ako objednávateľa, tak aby mohol poskytovať žiadané služby pre verejného obstarávateľa v plnom rozsahu upravenom v opise predmetu zákazky. Podpora výrobcov pre súčasný HW a SW končí 31.8.2025, resp. 14.2.2026 viď príloha 10 SP (Základné informácie o IT prostredí NBS).

**Otázka č.10:**

V súbore priloha 10 SP (Zakladne informacie o IT prostredi NBS).docx v bode 9. píšete, že podpora poskytovaných služieb výrobcu a dodávateľa pre ThreatGuard je do 31.8.2025.

Otázka:

Je súčasťou služby aj dodávka licencií? Resp. máme ako možný poskytovateľ služieb naceniť aj dodanie licencií (Threat Intelligence)? Alebo si objednávateľ obstará licencie ThreaGuard v inom obstarávaní?

**Odpoveď:**

Predmetom zákazky nie je dodanie akýchkoľvek licencií pre verejného obstarávateľa ako budúceho objednávateľa. Povinnosťou budúceho poskytovateľa je v rámci poskytovaných služieb zabezpečiť si všetky potrebné licencie, tak aby mohol poskytovať žiadané služby pre verejného obstarávateľa v plnom rozsahu upravenom v opise predmetu zákazky.

**Otázka č.11:**

Z dôvodu efektívnosti a úspory finančných prostriedkov objednávateľa, zabezpečí objednávateľ prístupy v rámci súčasnej exit služby od stávajúceho poskytovateľa pre oblasť contentu (LM, EDR, NDR, SIEM a ostatných technológií) nástroja pre nového poskytovateľa?

**Odpoveď:**

Áno.

**Otázka č.12:**

V prílohe č.7 Zoznam špecifických use caseov.docx, sú jednotlivé use case vymenované.

Je možné sa prihlasovať bez overenia cez AD?

* detekcia prihlásení na Oracle privilegované účty mimo pracovnú dobu
* detekcia neúspešných prihlásení na rôzne Oracle účty z rovnakej IP
* detekcia prihlásení na MSSQL privilegované účty mimo pracovnú dobu
* detekcia neúspešných prihlásení na rôzne MSSQL účty alebo inštancie z rovnakej IP
* detekcia neúspešných prihlásení na rôzne DAFNE účty z rovnakej IP
* detekcia prihlásení na DAFNE privilegované účty mimo pracovnú dobu
* používanie účtu používateľa počas jeho neprítomnosť
* nadmerný počet neúspešných prihlásení

Sú všetky administrátorské účty na AD?

Je možné vysvetliť skratky vPC a TU?

* detekcia vPC athentication failure
* detekcia TU athentication failure

Je pre bezpečnostný monitoring chcená detekcia malware odchádzajúcej pošty? Nechce poskytovateľ sledovať malware v prichádzajúcej pošte?

* detekcia malware v odchádzajúcej pošte

**Odpoveď:**

*Je možné sa prihlasovať bez overenia cez AD? Sú všetky administrátorské účty na AD?*

Na prihlasovanie do systémov v závislosti na ich charaktere sú využívané AD účty a prípadne aj lokálne účty.

*Je možné vysvetliť skratky vPC a TU?*

vPC – virtuálna pracovná stanica

TU – technický účet

*Je pre bezpečnostný monitoring chcená detekcia malware odchádzajúcej pošty? Nechce poskytovateľ sledovať malware v prichádzajúcej pošte?*

NBS prevádzkuje technológiu na skenovanie prichádzajúcej aj odchádzajúcej elektronickej pošty. Udalosti z tohto systému sú preposielané do SIEMu.

**Otázka č.13:**

v Prílohe č. 10 – Základné informácie o IT prostredí NBS\*\* je uvedené, že podpora poskytovaná výrobcom a dodávateľom pre všetky technológie SIEM vrátane LogRhythm, NetMon a Flowmon je platná do 31. 8. 2025. Zároveň je uvedené, že podpora ThreatGuard je taktiež platná do 31. 8. 2025 a Tenable do 14. 2. 2026.

Vzhľadom na to, že:

- plnenie zákazky má trvať po uzatvorení zmluvy až 48 mesiacov (t. j. hlboko za horizont uvedenej podpory), a cieľom zákazky je „zabezpečiť kontinuitu poskytovania služieb minimálne v súčasnej kvalite a rozsahu“,

žiadame o jednoznačné stanovisko zadávateľa k nasledujúcim otázkam:

1. Požaduje zadávateľ, aby boli všetky uvedené technológie (LogRhythm, Flowmon, Tenable, Trellix atď.) zachované aj počas trvania plnenia zákazky uchádzačom?

2. Požaduje zadávateľ, aby uchádzač zabezpečil výmenu (náhradu) technológií LogRhythm, Flowmon a ďalších systémov, u ktorých skončí podpora pred ukončením plnenia zákazky?

3. Ak áno, má uchádzač navrhnúť nové technológie už v rámci ponuky, alebo sa má výmena riešiť až v priebehu plnenia zákazky v koordinácii so zadávateľom?

4. V prípade, že výmena je požadovaná, je možné v ponuke predložiť funkčne rovnocenné alternatívy existujúcich technológií (napr. iný SIEM, NDR, EDR a pod.)?

Prosíme o priamu odpoveď: áno/nie

**Odpoveď:**

1. Nie
2. Podpora výrobcov pre súčasný HW a SW končí 31.8.2025, resp. 14.2.2026 viď príloha 10 SP (Základné informácie o IT prostredí NBS). Predmetom zákazky nie je nákup HW a SW pre verejného obstarávateľa ako budúceho objednávateľa. Predmetom zákazky je obstaranie služieb v plnom rozsahu upravenom v opise predmetu zákazky. Povinnosťou budúceho poskytovateľa je v rámci poskytovaných služieb zabezpečiť si všetok potrebný HW a SW do prostredia verejného obstarávateľa ako objednávateľa, tak aby mohol poskytovať žiadané služby.
3. Áno. Verejný obstarávateľ požaduje aby uchádzač v ponuke uviedol špecifikáciu technológií ktorými budú poskytované služby predmetu zákazky. Uvedené vyplýva z prílohy 9 Súťažných podkladov (Opis predmetu zákazky – Požiadavky na predmet zákazky).
4. Verejný obstarávate požaduje aby uchádzač uviedol vo svojej ponuke špecifikáciu technológií, ktorými budú poskytované obstarávané služby (SOC, SIEM, NDR, skener zraniteľností, BAS, sledovanie IT hrozieb zraniteľností) vrátane integrácií s bezpečnostnými systémami. Detailnejší popis je uvedený v prílohe 9 Súťažných podkladov Opis predmetu zákazky – Požiadavky na predmet zákazky. Obstarávateľ v tejto zákazke nebude realizovať náhradu existujúceho EDR riešenia iným alternatívnym riešením.

JUDr. Zuzana Jánošová

Vedúca, oddelenie centrálneho obstarávania

Mgr. Tomáš Lepieš

Riaditeľ, odbor hospodárskych služieb

1. Samostatný dokument – príloha č. 1 [↑](#footnote-ref-1)