

## Záujemcovia

Váš list číslo/zo dňa	Naše číslo	Vybavuje/kontakt	Dátum
	SE_KYB_SLU	Mgr. Michaela Takáč Markovičová +421 918 763 477	28.10.2022

Vec

### Vysvetlenie informácií potrebných na vypracovanie ponuky

Mesto Senica, so sídlom Štefánikova 1408/56 90525 Senica (ďalej len „verejný obstarávateľ“) uverejnil vo Vestníku verejného obstarávania č. 224/2022 z 17.10.2022 pod zn. 43897-WNS Výzvu na predkladanie ponúk (ďalej len „Výzva“) na predmet zákazky „Expertné služby pre bezpečnosť IT systémov“.

**Verejný obstarávateľ Vám v súlade so zákona č. 343/2015 o verejnom obstarávaní (ďalej len „ZVO“) poskytuje vysvetlenie informácií potrebných na vypracovanie ponuky.**

**Otázka č. 1:** Otázka pre oblasť popisu východiskového stavu:

Verejný obstarávateľ nakúpil nasledovné HW a SW prvky pre bezpečnosť IKT infraštruktúry:

- LOGmanager-M od spoločnosti LOGmanager
- 2 ks firewall Palo Alto Networks PA-450 od spoločnosti Palo Alto Networks
- 130 antivírusových licencií Endpoint Security Complete od spoločnosti Symantec

Bude potrebné všetky tieto prvky implementovať v prostredí infraštruktúry verejného obstarávateľa. Znamená to, že uvedené HW a SW prvky nie sú nasadené v prostredí verejného objednávateľa?

**Odpoveď č. 1:** Áno, bude potrebné všetky tieto prvky implementovať v prostredí infraštruktúry

**Otázka č. 2:** Otázky pre oblasť: Implementácia centrálneho logovacieho systému od výrobcu LOGmanager, zariadenie LOGmanager – M.

Objednávateľ požaduje konfiguráciu Windows a Linux systémov pre zasielanie logov do systému.

Môže objednávateľ upresniť o aký počet Windows a Linux systémov sa jedná?

**Odpoveď č. 2:** Predmetom zákazky je uzavretie rámcovej dohody na základe ktorej bude verejný obstarávateľ objednávať konkrétne služby. Bližšie informácie budú upresnené úspešnému uchádzačovi vzhľadom na to, že predmetom VO sú konkrétne počty človekodní.

**Otázka č. 3:** Otázky pre oblasť: Implementácia Firewallu 2x Palo Alto Networks PA-450

- Na akých firewalloch je prevádzkované aktuálne riešenie (výrobca a typ)?
- Bude pri migrácii k dispozícii kompletný konfiguračný súbor zo súčasných firewallov?
- Je požadovaná migrácia a revízia komunikačných pravidiel zo súčasného riešenia na nové riešenie. O aký približný počet komunikačných pravidiel sa jedná?
- Objednávateľ požaduje odsegmentovanie PROD a TEST prostredí. Koľko VLAN je v súčasnosti

využívaných v PROD a TEST prostredí? Koľko nových VLAN s komunikačnými pravidlami bude požadovaných pri implementácii?

- Bude dostupná klasifikácia dát pred implementáciou DLP do PaloAlto?

**Odpoveď č. 3: Predmetom zákazky je uzavretie rámcovej dohody na základe ktorej bude verejný obstarávateľ objednávať konkrétne služby. Bližšie informácie budú upresnené úspešnému uchádzačovi vzhľadom na to, že predmetom VO sú konkrétne počty človekodní. Verejný obstarávateľ ma za to, že niektoré informácie sú citlivého charakteru a budú sprístupnené úspešnému uchádzačovi.**

**Otázka č. 4:** Otázky pre oblasť: Implementácia Ochrany koncových staníc 130x Symantec Endpoint Security Complete

- Aká ochrana koncových staníc je využívaná v súčasnosti?
- Na koľkých koncových staniciach a serveroch je nasadené súčasné riešenie ochrany koncových staníc?

**Odpoveď č. 4: Predmetom zákazky je uzavretie rámcovej dohody na základe ktorej bude verejný obstarávateľ objednávať konkrétne služby. Bližšie informácie budú upresnené úspešnému uchádzačovi vzhľadom na to, že predmetom VO sú konkrétne počty človekodní. Verejný obstarávateľ ma za to, že niektoré informácie sú citlivého charakteru a budú sprístupnené úspešnému uchádzačovi.**

**Otázka č. 5:** Otázky pre oblasť: Pravidelné služby bezpečnostného analytika

- Objednávateľ požaduje od dodávateľa nasadenie vlastného SIEM riešenia alebo požaduje využívanie zariadení, ktoré sú v sieti nasadené (napríklad LOGmanager)?
- Objednávateľ v podmienkach píše: „Pomocou SIEM budú konzultanti SOC nepretržite monitorovať bezpečnostné incidenty a budú zodpovední za reakciu, ak sa zistí.“ To znamená, že objednávateľ požaduje 24x7 SOC službu? Vie objednávateľ definovať SLA parametre pre túto službu (napríklad čas detekcie, analýzy, investigácie, reakcie,...)?
- Objednávateľ definoval nasledovné dotknuté systémy:
  - o isvs\_10862 Komplexný informačný systém mesta Senica,
  - o isvs\_10863 Informačný systém personalistiky a miezd mesta Senica,
  - o isvs\_10864 Webový portál mesta Senica,
  - o svs\_10865 Systém elektronickej pošty mesta Senica

Ktorý z uvedených dotknutých systémov mesta využíva prostredia spomínané v službách bezpečnostného analytika (ako sú Office365, SalesForce.com, Amazon Web Services (AWS), Azure a Google Cloud)?

**Odpoveď č. 5: Obstarávateľ požaduje využívanie zariadení, ktoré sú v sieti nasadené.**

**SIEM konzultanti budú notifikovaný o bezpečnostných incidentoch v reálnom čase, pričom požadovaná reakcia na incident je v najnižšom možnom čase pre minimalizáciu škody z nej vyplývajúcej, minimálne 8x5 s maximálnym časom reakcie do 2 hodín. 24x7 SOC služba nie je vyžadovaná.**

**Predmetom zákazky je uzavretie rámcovej dohody na základe ktorej bude verejný obstarávateľ objednávať konkrétne služby. Informácie o dotknutých systémoch budú upresnené v konkrétnej objednávke úspešnému uchádzačovi.**

**Otázka č. 6:** Otázky pre oblasť: Špecialista pre bezpečnosť informačných systémov

- Objednávateľ požaduje pravidelné testy zraniteľností. Je možné presnejšie časovo zadefinovať požadovanú pravidelnosť testov pre verejné a interné IP adresy?

**Odpoveď č. 6:** Predmetom zákazky je uzavretie rámcovej dohody na základe ktorej bude verejný obstarávateľ objednávať konkrétne služby. Bližšie informácie budú upresnené úspešnému uchádzačovi vzhľadom na to, že predmetom VO sú konkrétne počty človekodní.

**Otázka č. 7:**

Je potrebné spraviť aj expertízu, celý návrh dizajnu riešenia a následne aj implementáciu alebo máte záujem iba o dohľad nad implementáciou?

**Odpoveď č. 7:**

Je potrebné spraviť aj expertízu, celý návrh dizajnu riešenia a následne aj implementáciu. Bližšie informácie budú upresnené úspešnému uchádzačovi vzhľadom na to, že predmetom VO sú konkrétne počty človekodní.

**Otázka č. 8:**

Je možná práca vzdialene alebo osobne?

**Odpoveď č. 8:**

Niektoré služby budú musieť byť poskytované na mieste a v niektorých prípadoch ak to umožní predmet objednávky a nastavená bezpečnostná politika bude umožnený aj vzdialený prístup.

**Otázka č. 9:**

Je možná komunikácia v anglickom jazyku?

**Odpoveď č. 9:**

Nie

**Otázka č. 10:**

Je možné rozdeliť ponuku na časti (zvlášť Endpoint, FW, LOGmanager) alebo máte záujem o dodanie všetkých častí od jedného dodávateľa?

**Odpoveď č. 10:**

Obstarávateľ vyžaduje dodania celého rozsahu od jedného dodávateľa.

**Otázka č. 11:**

Aké všetky subscriptions má obstarávateľ zakúpené pre Palo Alto FW produkt?

**Odpoveď č. 11:**

Panorama central management software 25 devices, PA-450, Professional Subscription Bundle, PA-450, GlobalProtect subscription, PA-450, DLP subscription, PA-450, Partner enabled premium support, Partner enabled premium support 5 year prepaid, Panorama 25 devices

S pozdravom,

.....  
Mgr. Michaela Takáč Markovičová  
procesný garant