VÝZVA NA PREDLOŽENIE PONUKY (PRIESKUM TRHU)

podľa § 6 ods. 1 zákona č. 343/2015 Z. z. o verejnom obstarávaní

1. Názov predmetu zákazky

Vybavenie pracoviska SOC – Bezpečnostné nástroje (PHZ)

2. Druh zákazky

Dodanie tovarov

3. Identifikácia verejného obstarávateľa :

Obchodné meno / Názov	Národné centrum zdravotníckych informácií
Poštová adresa	Lazaretská 26, 811 09 Bratislava 1
IČO	00165387
Kontaktná osoba	Katarína Grejták Bednáriková
e-mail	Katarina.GrejtakBednarikova@nczisk.sk
adresa hlavnej stránky verejného obstarávateľa /URL/	www.nczisk.sk
Adresa zadávania zákazky /URL/ v systéme JOSEPHINE	https://josephine.proebiz.com/sk/tender/47389/summary

4. Stručný opis predmetu zákazky

Predmetom prieskumu je získanie indikatívnych cenových ponúk od relevantných hospodárskych subjektov na dodanie tovarov / bezpečnostných nástrojov pre vybavenie SOC pracoviska.

5. Spoločný slovník obstarávania

CPV podľa slovníka	Predmet
48000000-8	Softvérové balíky a informačné systémy
48730000-4	Softvérový balík na zaistenie bezpečnosti
48900000-7	Rôzne softvérové balíky a počítačové systémy

6. Lehota dodania:

Verejný obstarávateľ stanovuje lehotu plnenia pre jednotlivé položky v Prílohe č. 1.

7. Spôsob určenia ceny

(Indikatívna) cena za predmet zákazky musí byť stanovená v zmysle zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov. Navrhovaná cena musí byť v súlade s § 2 citovaného zákona o cenách založená na cene obchodného alebo sprostredkovateľského výkonu, ekonomicky oprávnených nákladoch a primeranom zisku.

Navrhovaná cena musí byť vyjadrená v eurách v súlade so zákonom č. 659/2007 Z. z. o zavedení meny euro v Slovenskej republike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Vyhlášok č. 97/ 2008 Z . z. a 75/2008 Z. z.

Návrh indikatívnej ceny musí obsahovať všetky predpokladané náklady spojené s plnením predmetu zákazky. Pri tvorbe cenovej ponuky je potrebné zohľadniť aj:

- primeranosť jej stanovenia na základe jemu vzniknutých nákladov a primeranosť zisku,
- požiadavky na plnenie predmetu zákazky v požadovaných lehotách a kvalite,

- lehoty dodania,
- súvisiace služby (ak aplikovateľné).

Verejný obstarávateľ požaduje predložiť vyplnenú / nacenenú Prílohu č. 2 tejto výzvy pri zohľadnení opisu predmetu zákazky uvedeného taktiež v Prílohe č. 1.

8. Možnosť predloženia variantných riešení:

Verejný obstarávateľ neumožňuje predložiť variantné riešenia.

9. Lehota na predkladanie ponuky

Lehota na predkladanie indikatívnych cenových ponúk je do: **03.10.2023 do 12.00 hod**.

10. Viazanosť/platnosť ponuky

Min. 3 mesiace odo dňa posledného dňa lehoty na predkladanie indikatívnych cenových ponúk.

11. Platobné podmienky

Platba bude realizovaná formou bezhotovostného platobného styku na základe daňového dokladu vystaveného poskytovateľom, splatnosť ktorého je do 60 kalendárnych dní odo dňa preukázateľného doručenia príslušnej faktúry verejnému obstarávateľovi/objednávateľovi. Verejný obstarávateľ neposkytuje preddavky, ani zálohové platby.

12. Spôsob predloženia indikatívnej ponuky

Prostredníctvom systému Josephine na linke uvedenej v bode 3 tejto výzvy, v prípade výpadku alebo technický problémov výnimočne aj elektronickou poštou na e-mailovú adresu uvedenú v bode 3 tejto výzvy.

Verejný obstarávateľ žiada hospodárske subjekty, aby vyplnili v rámci cenníka všetky riadky (položky), ktoré vie hospodársky subjekt dodať. Položky, ktoré nevie hospodársky subjekt dodať (nemá ich vo svojom portfóliu), ponechá nevyplnené (t. j. hospodársky subjekt môže predložiť indikatívnu cenovú ponuku aj len na niektoré vybrané položky).

13. Ďalšie súvisiace informácie:

Predloženie ponuky je indikatívne a do budúcna nekonštatuje konflikt záujmov a nebráni hospodárskemu subjektu zúčastniť sa zadávania zákazky na vyššie uvedený predmet zákazky po jeho vyhlásení.

Na základe predložených indikatívnych cenových ponúk v prieskume trhu zostaví Národné centrum zdravotníckych informácií ako verejný obstarávateľ v zmysle ZVO predpokladanú hodnotu zákazky, ktorá bude v ďalšom použitá na účely vypracovania analýzy nákladov a prínosov (CBA) pre projekt „Podpora budovania bezpečnostných dohľadových centier v prostredí verejnej správy“ v rámci výzvy MIRRI SR. Predmet zákazky bude v prípade úspešnosti projektu verejného obstarávateľa (spolu)financovaný z prostriedkov Plánu obnovy a odolnosti SR.

V Bratislave, dňa 25.9.2023

Prílohy:

- Príloha č. 1 – Opisu predmetu zákazky
- Príloha č. 2 – Štruktúrovaný rozpočet

Príloha č. 1 – Opis predmetu zákazky

Predmetom zákazky je dodanie špecializovaných bezpečnostných nástrojov pre vybavenie SOC pracoviska verejného obstarávateľa v rozsahu uvedenom nižšie.
V prípade konkrétnych technických a výrobných označení materiálov a zariadení takto špecifikovaných v tejto výzve, môže hospodársky v zmysle § 42 ods. 3 zákona o verejnom obstarávaní predložiť ponuku i na technický a/alebo funkčný ekvivalent (ak nie je uvedené inak).

Vybavenie pre forenznú analýzu

1. Nástroj pre digitálnu forenznú analýzu a správu elektronických dôkazov. Nástroj je určený pre účel zberu, analýzy a správy dát a vizualizáciu ich vzájomných vzťahov. Softvér určený pre forenznú analýzu s podporou súborových systémov Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) and FreeBSD's UFS2; Novell's NSS & NWFS; IBM's AIX jfs, JFS and JFS with LVm8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Palm, s podporou vyšetrovania emailovej komunikácie, podporou EnScript.
   Hlavný účel nástroja:
   - Zber dát bez ich zmeny a poškodenia zo zariadení a úložných médií, ako sú pevné disky, pamäťové karty, USB kľúče a ďalšie.
   - Hĺbková analýza digitálnych dát, vrátane vyhľadávania a identifikácie relevantných informácií.
   - Správa a katalogizácia digitálnych dát a ich bezpečné uloženie a archivácia pre forenznú analýzu.
   - Zabezpečenie integrity dát a dôkazov počas celého procesu forenzného vyšetrovania.
   - Vizualizácia vzťahov medzi dátami a ich analýza vo forme grafov a diagramov pre potreby vyšetrovania komplexných prípadov.
   - Vyhľadávanie a filtrovanie dát na základe rôznych kritérií, ako sú kľúčové slová, dátumy, typy súborov a ďalšie parametre.
   - Podpora analýzy dát z rôznych operačných systémov, vrátane Windows, macOS a rôznych distribúcií Linuxu.
   - Integrácia s ďalšími s ďalšími softvérovými nástrojmi a technológiami pre umožnenie rozšírenej funkcionality a efektívnej prácu s digitálnymi dátami.

   Napr. Encase Forensics alebo ekvivalentný
   Vrátane inštalačných a konfiguračných prác.
   Počet licencií: pre 2 používateľov
   Licenčné pokrytie: 36 mesiacov

2. Nástroj na extrakciu a analýzu dát z mobilných zariadení a digitálnych médií, dešifrovanie týchto dát a degenerovanie reportov. Vlastné napájanie, displej a podpora viacerých SIM kariet. Nástroj určený pre forenznú analýzu mobilných zariadení, tabletov, prehrávačov, GPS zariadení, SIM, smart hodiniek a podobne s podporou prístupu k živým, skrytím, alebo zmazaným údajom, integrovanou konzolou pre vývoj v jazyku Python a podporou operačných systémov Microsoft Windows 7 64-bit, 8.x 64-bit and 10 64-bit / Microsoft Windows 7 Boot Camp na zariadeniach Apple.
   Hlavný účel nástroja:
   - Logická a fyzická extrakcia systémových súborov alebo hesiel, či už zmazaných alebo chránených.
   - Kompletná extrakcia existujúcich, skrytých a vymazaných údajov: SMS, MMS, kontakty, história hovorov, kalendár, e-mail, médiá, informácie o polohe (WiFi, navigačné aplikácie, geotagy) a ďalšie.
   - Obchádzanie zámkou PIN/Pattern/Passcode z vybraných zariadení so systémom Android s akoukoľvek verziou.
   - Dešifrovanie v reálnom čase pre vybrané zariadenia.
   - Analýza mobilných zariadení iOS chránené heslom, jailbreak-nuté, non-jailbreak-nuté, šifrované a nešifrované iOS zariadenia.

   Napr. UFED Touch Ultimate Standard alebo ekvivalentný
   Vrátane inštalačných a konfiguračných prác.
   Počet licencií: pre 2 používateľov
   Licenčné pokrytie: 36 mesiacov

3. Forensic analytic tool for SIEM - On premise automatizovaný softvérový nástroj na riešenie analýzy existujúcich zdrojov udalostí z informáciami z rôznych zdrojov o útokoch, bežne dostupných informáciách o podozrivých aktivitách na Internete, informáciách zo sociálnych sietí, prípadne pre zber spravodajských informácií, kurátorstvo a obohatenie, ktoré pomáha bezpečnostným tímom rýchlo pochopiť kontext výstrah SIEM a SOAR. Musí obsahovať MITRE ATT&CK mapovanie, ktoré poskytuje okamžitý pohľad na globálne hrozby ovplyvňujúci stav zabezpečenia organizácie, analýzu vizuálnych

odkazov na rozšírenie k pridruženým modelom hrozieb vyššej úrovne. Taktiež musí obsahovať integrované sand-box riešenie, ktoré umožňuje podozrivé súbory pri vyšetrovaní umiestniť do karantény.
Vrátane inštalačných a konfiguračných prác.
Počet licencií: pre 600 užívateľov
Licenčné pokrytie: 36 mesiacov

Lehota dodania: do 30 kalendárnych dní odo dňa účinnosti zmluvy

Pentest lab

1. Skener zraniteľnosti - Nástroj na testovanie bezpečnosti webových aplikácií (Web Application Security Testing Tool), ktorý sa používa na identifikáciu a odstraňovanie bezpečnostných zraniteľností vo webových aplikáciách. Nástroj zabezpečuje automatizáciu počas životného cyklu vývoja softvérových riešenie (SDLC). Softvérový nástroj pre penetračné testovanie s podporou testov PHP, ASP, J2EE, testovania zraniteľností vo webových formulároch, testovania cookies.
   Účelom nástroja je automatizované skenovanie webových aplikácií s cieľom odhaliť rôzne druhy bezpečnostných zraniteľností, vrátane:
   - SQL Injection (SQLi): Vykonanie neoprávnených SQL dopyty na databázu.
   - Cross-Site Scripting (XSS): Možnosti vkladania škodlivého kódu do webovej stránky, ktorý by mohli byť vykonané v prehliadači koncového používateľa.
   - Cross-Site Request Forgery (CSRF): Vytváranie nežiaducich žiadosti v mene koncového používateľa.
   - Bezpečnostné chyby v autentifikácii a autorizácii: Hľadá nedostatočnú autentifikáciu, autorizáciu a kontrolu prístupu.
   - Nedostatočné ošetrenie vstupov, chyby vo vývoji a ďalšie.

   Napr.: Invicti alebo ekvivalent.
   Vrátane inštalačných a konfiguračných prác
   Počet licencií: na 2 používateľov
   Licenčné pokrytie: 36 mesiacov.

2. Nástroj na simuláciu red team - Nástroj na simuláciu protivníka a operácii červeného tímu, ako spôsob hodnotenia bezpečnosti, ktoré replikujú taktiku a techniky pokročilého protivníka v sieti tzv. "red teaming" alebo "adversary simulation," pri ktorých bezpečnostné tímy, alebo iné organizácie testujú svoju vlastnú bezpečnosť pomocou nástrojov a taktík, ktoré by mohli použiť skutoční útočníci.
   Hlavný účel nástroja:
   - Umožňuje útočníkom pristupovať k cieľovým systémom a sieťam. Môže byť použitý na prekonanie obranných mechanizmov, ako sú firewally alebo antivirusové programy.
   - Umožňuje útočníkom skákať cez viacero systémov a maskovať svoju prítomnosť, čím sa zvyšuje náročnosť detegovania ich aktivity.
   - Umožňuje meniť indikátory siete tak, aby zakaždým vyzerali ako iný malvér.
   - Zber informácii o cieľovom prostredí, vrátane informácií o systémových konfiguráciách a zraniteľnostiach.
   - Exfiltrácia údajov z cieľového systému alebo siete.

   Napr.: Cobaltstrike alebo ekvivalent.
   Vrátane inštalačných a konfiguračných prác
   Počet licencií: na 3 používateľov
   Licenčné pokrytie: 36 mesiacov.

Lehota dodania: do 30 kalendárnych dní odo dňa účinnosti zmluvy

Malvér lab

1. SW pre reverzné inžinierstvo - Nástroj automatizovaného reverzného inžinierstva na analýzu softvérových aplikácií, zdrojového kódu a iných digitálnych entít za účelom pochopenia ich fungovania, identifikácie zraniteľností a iných bezpečnostných rizík.
   Pokročilá analýza malware: SW nástroj musí umožňovať zachytávanie časových úsekov úplného spustenia systému (CPU, pamäť, hardvérové udalosti), aby poskytla jedinečné analytické funkcie, ktoré urýchlia a rozšíria proces reverzného inžinierstva. Požaduje sa podpora pre integráciu s IDA a Wireshark
   Požaduje sa licencia pre 1xnamed používateľa s 1 Record & 1 Replay, 1 Analysis (1 GUI + 1 Script) s podporou operačného systému MS Windovs a Linux s podporou min. Trace View, Taint View, Memory

View, Strings View, Search View, CPU View, Backtrace View, OS Specific Info. (OSSI), Framebuffer View, Axion (GUI) po dobu 36 mesiacov.
Účel nástroja:
- Statická analýza zdrojového kódu analýzou binárne súbory bez jeho spúšťania pre potreby identifikácie škodlivých kódov, zraniteľností a ďalších aspektov bezpečnosti.
- Dynamická analýza zdrojového kódu sledovaním jeho správania v reálnom čase.
- Identifikácia zraniteľností a potenciálnych hrozieb v zdrojovom kóde.
- Detekcia malvéru a škodlivého softvéru v binárnych súboroch.
- Rozklad kódu pre potreby preverenia funkčnosti aplikácie, vrátane identifikácie funkcií, prenosov údajov.

Napr. Tetrane alebo ekvivalent
Vrátane inštalačných a konfiguračných prác
Počet licencií: na 2 používateľov.
Licenčné pokrytie: 36 mesiacov.

2. Disassembler a dekompiler na x64 platformu - Nástroj reverzného inžinierstva a analýzy binárneho kódu pre prácu s binárnym kódom a disassemblovaním programov. Analýza malware: dokáže vytvárať mapy ich vykonávania, ktoré zobrazujú binárne inštrukcie, ktoré procesor skutočne vykonáva v symbolickej reprezentácii (v jazyku assembleru). Dissasembler poskytuje pokročilé techniky, aby dokázala generovať zdrojový kód v jazyku assembleru zo strojovo spustiteľného kódu a aby bol tento zložitý kód čitateľnejší pre človeka. Požadované parametre zahŕňajú podporu pre lokálny a vzdialený debugging, dekompiler pre x64 platformu, skriptovanie na automatizáciu.
   Hlavnými účelom nástroja je:
   - Možnosť prekladu binárneho kódu programu do ľudsky čitateľného assemblerového kódu pre účel analýzy funkčnosti a správania programu.
   - Statická analýza disassemblovaného kódu a hľadanie rôznych typov chýb, bezpečnostných zraniteľností, malvéru a ďalších problémov.
   - Použitie grafického používateľského rozhrania, ktoré umožňuje vizuálne prechádzať a analyzovať disassemblovaný kód a interagovať s ním
   - 2x floating license + 2x x64 dekompiler.

   Napr. IDA Pro + 64bit dekompiler alebo ekvivalent
   Vrátane inštalačných a konfiguračných prác
   Počet licencií: na 2 používateľov
   Licenčné pokrytie: 36 mesiacov.

3. Sandbox - Nástroj, ktorý umožňuje analýzu škodlivého softvéru a jeho správanie v izolovanom a bezpečnom prostredí resp. detekciu škodlivého softvéru, ktorý spúšťa podozrivý objekt vo virtuálnom stroji (VM) s plne funkčným operačným systémom a zisťuje škodlivú aktivitu objektu analýzou jeho správania. Ak objekt vykonáva škodlivé akcie vo virtuálnom počítači, karanténa ho deteguje ako malvér. Hlavný účel nástroja:
   - Automatizácia procesu analýzy malvéru formou vykonávania testov a skenovaní nad škodlivým softvérom pre identifikáciu správania sa malvéru, zistenia rozsahu vykonávaných aktivít malvérom a rozsahu možných systémových zmien.
   - Izolácia škodlivého softvéru od skutočného prostredia, čím sa minimalizuje riziko šírenia infekcie alebo poškodenia skúmaného systému.
   - Sledovanie správania malvéru v kontrolovanom prostredí a analýza jeho interakcie s operačným systémom, súbormi a sieťovou komunikáciou. Tieto informácie pomáhajú bezpečnostným expertom pochopiť, aký je účel malvéru a aké sú jeho ciele.
   - Generovanie záznamov z analýzy pre lepšie porozumenie hrozbám a vyvinutie stratégie na ich ochranu a odstránenie.
   - Integrácia s inými bezpečnostnými nástrojmi a riešeniami na zlepšenie detekcie a reakcie na hrozby.
   - Výsledkom použitia je lepšie porozumenie škodlivému softvéru, jeho charakteristikám a rizikám, ktoré predstavuje. To umožní organizácii zlepšiť svoju bezpečnosť a rýchlo reagovať na nové hrozby.

   Napr. Automated Malware Analysis & Sandbox: Falcon Sandbox alebo ekvivalent
   Vrátane inštalačných a konfiguračných prác
   Počet licencií - licencovanie na počet kontrolovaných súborov: do 300 súborov mesačne
   Licenčné pokrytie: 36 mesiacov.

4. Malware analytic tool for SIEM - Vyhľadávanie v súbore údajov VirusTotal vzorky malvéru, adresy URL, domény a adresy IP podľa binárnych vlastností, verdiktov antivírusovej detekcie, statických funkcií, vzorcov správania, ako je komunikácia s konkrétnymi hostiteľmi alebo adresami IP, metaúdaje

odosielania a mnoho ďalších pojmov. Podporuje označenie súborov podobných podozrivému, ktorý sa skúma. Vzorky zodpovedajúce vyhľadávacím kritériám je možné stiahnuť.
Napr. Virustotal alebo Exodus intelligence alebo ekvivalent
Vrátane inštalačných a konfiguračných prác
Počet licencií: licencovanie na počet požiadaviek do 500 mesačne / prípadne PRO verziu s ročnou licenciou
Licenčné pokrytie: 36 mesiacov

5. Honeypot - Nástroj na detekciu, monitorovanie a zbieranie informácií o kybernetických útočníkoch a hrozbách v informačných systémoch formou vytvárania falošného cieľa pre útočníkov. Ide o systém, ktorý nepredstavuje priamu produkčnú hodnotu a jeho hlavným cieľom je umožniť útočníkovi istý druh prieniku s následnou možnosťou analýzy jeho činnosti. Účel:
   - Detekcia útokov zaznamenávaním všetkých aktivít útočníkov, ktorí sa pokúšajú zneužiť falošnú službu alebo systém. Týmto spôsobom umožňujú bezpečnostným tímom sledovať a analyzovať nové a existujúce kybernetické hrozby.
   - Zber dôležitých informácií o technikách, nástrojoch a taktikách používaných útočníkmi. Tieto informácie môžu byť následne použité na zlepšenie bezpečnostných opatrení a obrany organizácie.
   - Aktivity útočníkov na honeypotoch s cieľom odhaliť ich zraniteľnosti a slabiny umožňuje dozvedieť sa, aké časti jej siete alebo systému sú najviac ohrozené.
   - Izolácia útočníkov a ich odstránenie z reálnej siete. Tým sa minimalizuje riziko pre skutočné systémy a umožňuje bezpečnostnému tímu čas na reakciu.

   Vrátane inštalačných a konfiguračných prác
   Počet licencií: na 20 trapov
   Licenčné pokrytie: 36 mesiacov.

Lehota dodania: do 30 kalendárnych dní odo dňa účinnosti zmluvy

Príloha č. 2 – Štruktúrovaný rozpočet

P. č.	Názov	Požadované technické parametre a licenčné pokrytie	Navrhovaný/ocenený produkt (výrobca, značka, názov príp. produktu) *VYPLNÍ HOSPODÁRSKY SUBJEKT*	M. j.	Množstvo	Jednotková cena v € bez DPH	Jednotková cena v € s DPH	Celková cena v € bez DPH	Celková cena v € s DPH
Forenzný lab									
1.	Nástroj pre digitálnu forenznú analýzu a správu elektronických dôkazov	Viď príloha č. 1 – Opis predmetu zákazky		Kus	3	- €	- €	- €	- €
2.	Nástroj na extrakciu a analýzu dát z mobilných zariadení a digitálnych médií			Kus	1	- €	- €	- €	- €
3.	Forensic analytic tool for SIEM			Kus	1	- €	- €	- €	- €
Pentest lab									
1.	Skener zraniteľnosti	Viď príloha č. 1 – Opis predmetu zákazky		Kus	1	- €	- €	- €	- €
2.	Nástroj na simuláciu red team			Kus	1	- €	- €	- €	- €
Malvér lab									
1.	SW pre reverzné inžinierstvo	Viď príloha č. 1 – Opis predmetu zákazky		Kus	1	- €	- €	- €	- €
2.	Disassembler a dekompiler na x64 platform			Kus	1	- €	- €	- €	- €
3.	Sandbox			Kus	1	- €	- €	- €	- €
4.	Malware analytic tool for SIEM			Kus	1	- €	- €	- €	- €
5.	Honeypot			Kus	1	- €	- €	- €	- €
	CELKOM							**- €**	**- €**