

Smluvní strany

ALTEPRO solutions a.s.

IČO: 03665496

DIČ: CZ03665496

Sídlem: Na Maninách 1092/20, Holešovice, 170 00 Praha 7

Bankovní spojení: Komerční banka, číslo účtu: 107-9161070297/0100

Spisová značka: B 20333 vedená u Městského soudu v Praze

Jednající: Ing. Martin Vitek, člen představenstva

Kontaktní osoba: Jan Pekar, key account manager

Telefon: 603 865 986; Email: jan.pekr@altepro.cz

dále jen jako „**dodavatel**“ na straně jedné

a

Národní centrum ošetrovatelství a nelékařských zdravotnických oborů

IČ: 00023850

DIČ: CZ00023850

Sídlem: Vinařská 965/6, Brno, PSČ 603 00

Zastoupený: PhDr. Mgr. Michaela Hofštetrová Knotková, ředitelka

Bankovní spojení: KB Brno, číslo účtu: 87439621/0100

Kontaktní osoba: Mgr. Vojtěch Pilar

Telefon: +420 543 559 254, Email: pilar@nconzo.cz

dále jen jako „**objednatel**“ na straně druhé

se v souladu s ustanovením § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, dohodly níže uvedeného dne, měsíce a roku tak, jak stanoví tato

KUPNÍ SMLOUVA

(dále jen „**Smlouva**“)

Preambule

Tato kupní smlouva se uzavírá na základě výsledku zadávacího řízení na podlimitní veřejnou zakázku zadávanou podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, s ohledem na znění § 53 a ve spojení s § 6 tohoto zákona, s názvem „NCO NZO Brno – Systémová ochrana 2022“ (ID zakázky: VZ0149985). Dodavatel byl vybrán objednatelem v souladu s hodnotícími kritérii stanovenými v zadávacích podmínkách.

1. Předmět smlouvy

- 1.1. Předmětem této smlouvy je zajištění dodávky softwarového řešení nástroje pro ochranu před škodlivých kódem ve smyslu § 21 dle vyhlášky č. 82/2018 Sb. (VoKB), resp. § 5 odst. 3) písm. e) zákona 181/2014 Sb. (ZoKB) nástroj pro ochranu před škodlivých kódem. Součástí plnění je zajištění všech činností souvisejících se zajištěním požadovaných služeb a dodávky předmětu zakázky.
- 1.2. Předmětem této smlouvy je zejména závazek dodavatele dodat IT komponenty, kde bližší specifikace dodávky včetně specifikace technické je přílohou č. 1A a 1B této smlouvy (dále jen „Zboží“), převést vlastnické právo ke Zboží na objednatele, a závazek objednatele uhradit dodavateli za dodané Zboží dohodnutou kupní cenu. Dodavatel se zavazuje dodat objednateli Zboží a poskytnout související služby do místa plnění.

2. Kupní cena a platební podmínky

- 2.1. Kupní cena Zboží dle této smlouvy byla stanovena dohodou smluvních stran následovně:
 - a) 1. etapa projektu: Poskytnutí licencí
= 1.852.825,00 Kč bez DPH
 - b) 2. etapa projektu: Podpora provozu
= 5.000,00 Kč bez DPH měsíčně
 - c) 3. etapa projektu: Podpora implementace v prostředí zákazníka
= 20.000,00 Kč bez DPH za jeden člověkodenní poskytování podpory při implementaci v prostředí zákazníkaKe sjednané ceně bude připočtena DPH v zákonné výši.
Podrobná specifikace ceny Zboží a souvisejících služeb je uvedena v příloze č. 2 této smlouvy.
- 2.2. Kupní cena je stanovena jako nejvýše přípustná, konečná, neměnná za jinak nezměněných podmínek a zahrnuje všechny náklady související s předáním Zboží. Kupní cena zahrnuje rovněž veškeré náklady, přiměřený zisk a obsahuje započtená rizika včetně finančních vlivů jako je např. inflace po celou dobu realizace zakázky. Ceny zahrnují veškeré náklady dodavatele související s realizací předmětu veřejné zakázky. Kupní cena může být měněna pouze v případě, pokud po podpisu smlouvy dojde ke změnám sazeb DPH.
- 2.3. Daňový doklad bude vystaven až po řádném doručení a převzetí Zboží či souvisejících služeb ze strany objednatele, a to na základě skutečně odebraných služeb za uplynulé období.
- 2.4. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.
- 2.5. Kupní cena je splatná ve lhůtě 21 dnů ode dne doručení daňového dokladu objednateli. Splatností se rozumí odepsání finančních prostředků z účtu objednatele.
- 2.6. Objednatel souhlasí se zasíláním elektronických daňových dokladů od zhotovitele ve formátu *.pdf, odpovídajících příslušným ustanovením zákona o DPH.
- 2.7. Faktura musí obsahovat náležitosti stanovené příslušnými právními předpisy, a to zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění platném k datu uskutečnění zdanitelného plnění, a zákonem č. 563/1991 Sb., o účetnictví, ve znění platném k témuž datu. Přílohou faktury bude kopie protokolu o předání Zboží, či o poskytnutí služeb.
- 2.8. V případě, že zasláná faktura nebude mít náležitosti daňového dokladu nebo na ní nebudou uvedeny údaje specifikované v této smlouvě, nebo bude neúplná a nesprávná, je jí objednatel oprávněn vrátit dodavateli k opravě či doplnění a nedostává se do prodlení s úhradou kupní ceny. Od doručení opravené faktury začíná běžet nová lhůta splatnosti.

3. Dodací podmínky

- 3.1. Dodavatel se podpisem této smlouvy zavazuje dodat objednateli v souladu s touto smlouvou Zboží specifikované v čl. 1.2 této smlouvy a převést na objednatele právo užití k tomuto Zboží. Zboží bude předáno ve formě zpřístupnění licenčních klíčů.
- 3.2. Dodavatel po dobu trvání této smlouvy v obvyklé pracovní době zajistí následující související služby spojené s dodávkou Zboží:
 - a) technickou podporu implementace dodávaného řešení dle specifikace v příloze č. 1A a 1B této Smlouvy,
 - b) technickou podporu provozu dodávaného řešení dle specifikace v příloze č. 1A a 1B této Smlouvy.
- 3.3. Harmonogram plnění je následující:
 - d) 1. etapa projektu: Poskytnutí licencí
 - a. Licence budou poskytnuty nejpozději k datu 21.11.2022 a budou platné na období 5 let.
 - b. Poskytnutí licencí skrze licenční portál výrobce je prvním fakturačním milníkem.
 - c. Ze strany objednatele bude stvrzen bezprostředně po poskytnutí licencí skrze licenční portál výrobce Akceptační protokol, na jehož základě je oprávněn dodavatel fakturovat.
 - e) 2. etapa projektu: Podpora provozu
 - a. Měsíční rozsah této podpory představuje objem prací na úrovni 1 člověkodne v měsíci.
 - b. Fakturace bude probíhat na měsíční bázi vždy za předchozí měsíc.
 - c. Dodavatel fakturuje pravidelně vždy k poslednímu dni měsíce, ve kterém byly služby poskytnuty.
 - d. V případě, že služba nebyla poskytována po celý měsíc, pak náleží dodavateli alikvotní část ze smluvní měsíční odměny.
 - f) 3. etapa projektu: Podpora implementace v prostředí zákazníka
 - a. Poskytnutí konzultační aktivity a poradenství pro pracovníky zadavatele ve vztahu k nasazení bezpečnostních agentů na koncové stanice a servery bude probíhat po dobu prvních 3 měsíců po poskytnutí licencí
 - b. Rozsah podpory implementace: maximálně 10 člověkodní
 - c. Fakturace proběhne po protokolárním dokončení implementace, či po vyčerpání celkového rozsahu implementace. Ze strany objednatele bude stvrzen bezprostředně po dokončení implementace či vyčerpání celkového rozsahu implementace Akceptační protokol, na jehož základě je oprávněn dodavatel fakturovat.
- 3.4. Místem plnění je sídlo zadavatele: Vinařská 965/6, 603 00 Brno.

4. Prohlášení dodavatele

- 4.1. Dodavatel prohlašuje, že Zboží, jehož dodání je předmětem této smlouvy, má vlastnosti uvedené v této smlouvě, zejména v její příloze č. 1A, a vlastnosti, které jsou pro takové zboží obvyklé.

- 4.2. Dodavatel dále prohlašuje, že Zboží, jehož dodání je předmětem této smlouvy, splňuje relevantní technické, hygienické, veterinární, bezpečnostní a další standardy dle předpisů Evropské Unie a odpovídá požadavkům stanoveným právními předpisy České republiky.

5. Přechod užívacího práva

- 5.1. Užívací právo k softwarovému řešení nástroje pro ochranu před škodlivým kódem, přechází na objednatele ke dni poskytnutí licencí skrze licenční portál výrobce.

6. Záruka za jakost a záruční servis

- 6.1. Dodavatel poskytuje objednateli záruku za jakost Zboží ve smyslu ustanovení § 2113 a násl. občanského zákoníku.
- 6.2. Doba trvání záruky je uvedena v příloze č. 1 této smlouvy. Zboží je kryto technickou podporou výrobce na shodné období.
- 6.3. Veškeré vady, na které se vztahuje záruka, je objednatel oprávněn oznámit dodavateli písemně, telefonicky nebo e-mailem (dále jen „reklamace“). Objednatel je oprávněn oznámit dodavateli vadu Zboží kdykoli až do uplynutí záruční doby.
- 6.4. Dodavatel garantuje, že v rámci poskytnuté licence ke Zboží, je v případě vady objednatel oprávněn kontaktovat technickou podporu výrobce, a to prostřednictvím technické podpory dodavatele, a má nárok na instalaci a implementaci opravy (patch, hot-fix, případně upgrade) ke Zboží, pokud výrobce takovou buď uvolní k užívání svým zákazníkům.

7. Sankce

- 7.1. Smluvní strany sjednají smluvní pokutu ve výši 0,05 % z dlužné částky za každý započatý den prodlení se zaplacením daňového dokladu.

8. Řešení sporů, rozhodné právo

- 8.1. Smluvní strany vynaloží veškeré úsilí k tomu, aby vyřešily všechny spory, které by mohly vzniknout v souvislosti s touto smlouvou a její realizací v první řadě vzájemnou dohodou.
- 8.2. Smluvní strany se dohodly, že tato smlouva a práva a povinnosti z ní vyplývající se řídí a vykládají v souladu se zákony České republiky, zejména s příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
- 8.3. Objednatel si vyhrazuje právo od smlouvy odstoupit bez uvedení důvodu s maximálně tříměsíční výpovědní lhůtou bez finančního vyrovnání za služby, jejichž plnění by nastalo po lhůtě odstoupení od smlouvy.

9. Závěrečná ustanovení

- 9.1. Smlouva nabývá platnosti dnem jejího podpisu posledním z účastníků této smlouvy.
- 9.2. Smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv. Objednatel je zodpovědný za řádné zveřejnění smlouvy v registru smluv. Objednatel bude dodavatele informovat bezprostředně po té, co bude smlouva uveřejněna v registru smluv.

- 9.3. Smlouva se uzavírá na období 5 let ode dne její účinnosti.
- 9.4. Obě smluvní strany souhlasí se zveřejněním všech náležitostí smluvního vztahu založeného touto smlouvou.
- 9.5. Nedílnou součástí této smlouvy jsou tyto její přílohy:
- a) Příloha č. 1A: Technická specifikace plnění dle přílohy č. 6 zadávacích podmínek veřejné zakázky
 - b) Příloha č. 1B: Technická specifikace plnění - popis účastníka zadávacího řízení
 - c) Příloha č. 2: Výpočet nabídkové ceny
 - d) Příloha č. 3: Zadávací dokumentace veřejné zakázky
- 9.6. Smlouva je vyhotovena ve dvou stejnopisech, z nichž každá smluvní strana obdrží po jednom stejnopisu.
- 9.7. Smluvní strany na závěr této smlouvy výslovně prohlašují, že jim nejsou známy žádné okolnosti bránící v uzavření této smlouvy.
- 9.8. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, a shledaly, že její obsah přesně odpovídá jejich pravé a svobodné vůli a zakládá právní následky, jejichž dosažení svým jednáním sledovaly, a proto ji níže, prosty omylu, lsti a tísně, jako správnou podepisují.

Dodavatel:

Objednatel:

V Praze dne

V Brně dne

.....
ALTEPRO solutions a.s.
Ing. Martin Vítek
člen představenstva

.....
**Národní centrum ošetřovatelství a
nelékařských zdravotnických oborů**
PhDr. Mgr. Michaela Hofštetrová Knotková
ředitelka

Příloha č. 1A Smlouvy:

Technická specifikace plnění dle přílohy č. 6 zadávací dokumentace

EDR systém pro koncové stanice

Technické požadavky na EDR pro koncové stanice

- Podpora Windows (Windows 7 a novější, včetně Windows Server) a MacOS 10.13 a novější.
- Podpora nasazení ve virtualizovaném prostředí
- Centrální management konzole celého řešení umístěná v cloudovém prostředí výrobce řešení
- Rozhraní agenta na koncové stanici v českém jazyce, zprávy lze plně upravit případně přeložit do jiného jazyka (například upozornění typu „nalezen virus“).
- Napojení na Active Directory
- Instalace základního agenta a následné doinstalování zbylých modulů díky již provedené instalaci
- Agent potřebuje hesla pro jeho deaktivaci a odinstalování (volitelně)
- Rozdělení politiky na stav, kdy je agent on-site a kdy je mimo firmu
- Instalace pomocí MSI balíčku nebo automatizovaného web instalátoru, podpora bezobslužné instalace
- Agent tvoří jeden, maximálně 2 instalační balíky na koncové stanici – tj. endpoint klient + EDR
- Možnost plnohodnotné integrace do XDR
- Moduly endpoint agenta:
 - Firewall
 - Stavový firewall na úrovni síťové karty
 - Možnost nastavení priorit jednotlivých pravidel
 - Stavový firewall lze využít k izolaci klienta od sítě v případě napadení
 - Nastavení politiky, co vše má být na agentovi zakázáno/povoleno v případě „izolace agenta“ (například přístup k síťovým složkám, spouštění nových souborů, přístup k lokální složce na disku, specifické porty atd.), komunikace s managementem zachována
 - Reputace webu
 - Kontrola veškerého web provozu (nejen web browser)
 - Kontrola https URL pomocí pluginu v prohlížeči, že neprobíhá „Man In the Middle“ dešifrování a nahrazování certifikátu
 - Blokování web. komunikace na základě kategorizace (minimálně úroveň nebezpečné, vysoce podezřelé, podezřelé)
 - Možnost blokovat/neblokovat dosud nekategorizované/netestované stránky
 - White/black list na základě wildcards
 - Anti-malware:
 - Residentní ochrana
 - Smart Scan – optimalizace vytížení realtime skenu pomocí externí databáze signatur (cloud nebo on-premise)
 - Machine-learning engine – analýza souboru a jeho podobnosti s databází známých škodlivých/neškodných aplikací na základě několika charakteristik

daných souborů ve fázi ještě před spuštěním a následně i znovu po spuštění, na základě chování po spuštění

- Heuristická analýza
- Behavioralní analýza
 - Anti-ransomware (zablokuje proces provádějící neautorizované šifrování a obnoví datové soubory ze zálohy)
 - Automatický sken programů stažených přes email/web kanál – dotázání uživatele na spuštění takových programů v případě nízké reputace
- Ochrana proti rootkitům
- Skenování RAM na file-less malware, Cookies, skrytých složek
 - Sken komprimovaných souborů do min. 6. úrovně
 - Kontrola boot sektoru
 - Manual / real-time / scheduled scan
 - U manuálního a naplánovaného skenu nastavení využití CPU pro skenování (k dispozici jsou minimálně 3 úrovně – minimální z nich nemá vytížení CPU větší než 20 %)
 - Možnost využití whitelist databáze známého softwaru spravované výrobcem nabízeného řešení EDR pro snížení nároků anti-malware enginu
 - Možnosti omezit skenování na soubory
 - menší než X MB,
 - prvních Y souborů v komprimovaném archivu
 - Volba typů souborů, které budou skenovány
 - Podpora pro: ACCDB, ARJ, BAT, BIN, BOO, CAB, CHM, CLA, CLASS, COM, CSC, DLL DOC, DOCM, DOCX, DOT, DOTM, DOTX, DRV, EML, EXE, GZ, HLP, HTA, HTM, HTML, HTT, INI, JAR, JPEG, JPG, JS, JSE, LNK, LZH, MDB, MPD, MPP, MPT, MSG, MSO, NWS, OCX, OFT, OVL, PDF, PHP, PIF, PL, POT, POTM, PTX, PPAM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, PRC, RAR, REG, RTF, SCR, SHS, SYS, TAR, VBE, VBS, VSD, VSS, VST, VXD, WML, WSF, XLA, XLAM, XLS, XLSB, XLSM, XLSX, SLT, XLTM, XLTX, XML, Z, ZIP
 - Detekce typů podporovaných souborů na základě hlavičky, nikoliv názvu/přípony
 - Volba akce nad nákazou daného typu – malware, probable malware, CVE exploit, trojan atd.: clean, quarantine, pass, rename, delete plus možnost zálohy souboru před danou akcí
 - Skenování boot sektoru USB zařízení po vložení
 - Skenování všech souborů při vložení „výměnného zařízení“
- Independent mode – možnost povolení nezávislého provozu (nastavení se provádí lokálně, politiky nejsou přepisovány z management serveru)
- Množnost oddálit sken uživatelem
- Šifrovaná komunikace mezi agentem a serverem
- Agent kontaktuje server (stahování policy)
- Sandbox
 - Možnost přímého napojení na Sandbox s automatickým odesláním a analýzou podezřelých vzorků souborů
- Kontrola zařízení
 - Blokáce Autorun na USB

- Lze povolit/zakázat přístup na USB disky na základě výrobce disku, modelu i konkrétního sériového čísla. Součástí řešení je nástroj, který tyto informace o každém disku poskytne.
 - Lze zablokovat/povolit:
 - Bluetooth
 - COM
 - LPT
 - IEEE 1394
 - Infrared zařízení
 - Modemy
 - Bezdrátové síťové adaptéry
 - Mobilní zařízení
 - Lze povolit práva (Full, Modify, Read&Execute, Read, Block) pro datová úložiště, a to včetně volby konkrétního programu/procesu, který má tato práva udělena:
 - CD/DVD
 - Síťové disky
 - USB úložiště
- DLP
 - Skenování složek síťových úložišť
 - Možnost událost
 - logovat
 - upozornit uživatele na porušení politik
 - chtít po uživateli vepsat „zdůvodnění“ proč pokračovat
 - akci zablokovat
 - zvolit u kterých událostí budou „uložena“ i vlastní data (dokument) pro vyšetření incidentu
 - Volba přes jaké „kanály“ dochází k detekci události
 - tisk
 - CD/DVD
 - FTP
 - http/s
 - SMB
 - Směr „ze sítě ven“ / libovolný
 - ActiveSync
 - Email klient (např. Outlook)
 - Schránka v operační paměti
 - Možnost oddělit práva pro zobrazení DLP události a „vyšetřování“ DLP incidentu (vidět vlastní data, nad kterými DLP událost vznikla),
- Application control
 - Aplikace, které chci povolit nebo zakázat lze definovat na základě:
 - Specifické verze dané aplikace. Řešení už v sobě obsahuje databázi aplikací, jejich verzí i rozdělení do kategorií.
 - Sady „ověřených aplikací“ – např. pouze povolené verze Adobe Reader, Mozilla Firefox.
 - Typu aplikace (webový prohlížeč, hra, vývojářské nástroje, ovladače, ...), databáze součástí nástroje.

- Možnost ovlivnit, zda může aplikace spustit další aplikaci (další jedna úroveň) nebo libovolné množství aplikací (libovolná úroveň)
 - Cesty (string nebo regulární výraz)
 - Parametrů certifikátu (platnost/důvěryhodnost a parametry libovolné části C, L, CN, O, OU, ...)
 - Hash hodnoty (SHA1, SHA-256)
 - Možnost nástrojem určit hash hodnotu všech aplikací a tento seznam použít jako výchozí bod
- Možnost ovlivnit, zda může aplikace spustit další aplikaci (další jedna úroveň) nebo libovolné množství aplikací (libovolná úroveň)
- Host Intrusion Prevention (HIPS)
 - Intrusion Prevention systém na základě signatur, ochrana před síťovou exploitací, takzvaný virtual patching, obsahuje ochrany pro desktopové nasazení
 - Možnost fungování v módu detekce i prevence
 - Rozlišení ochrany na Exploit a Vulnerability
 - U jednotlivých pravidel odkaz dané ochrany na CVE, CVSS score, Microsoft atd.
 - Možnost nastavení výjimek pro IPS
- Kvalita nabízeného řešení:
 - Nabízené řešení, resp. jeho výrobce, musí být v mezinárodně platném benchmarkovém reportu pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“, přičemž předmětem benchmarkového reportu musí být EDR (Endpoint Detection and Response) technologie kybernetické bezpečnosti a benchmark musí obsahovat posouzení minimálně TOP10 celosvětových výrobců. (např. Gartner Magic Quadrant for Endpoint Protection Platforms)

EDR systém pro servery

Technické požadavky na EDR pro servery

Obecné vlastnosti:

- Komplexní zabezpečení fyzických, virtuálních a cloud serverů.
- Centrální management konzole celého řešení umístěná v cloudovém prostředí výrobce řešení
- Integrace s Amazon AWS, Microsoft Azure, Google Cloud, VMware vCenter, Microsoft AD – zobrazuje všechny fyzické, virtuální i cloud instance serverů a desktopů napříč organizací a je tak vidět ihned, které jsou chráněny a jakou politikou
- Možnosti automatizace pomocí API, pomocí nástrojů typu Ansible, Chef, Puppet
- Instalace možná pomocí instalačního balíčku (msi, rpm, deb...) nebo pomocí automatizovaného instalačního skriptu (powershell, bash), podpora bezobslužné instalace
- Správa uživatelů pro administraci na základě rolí
- Podpora SAML
- Podpora zabezpečení Docker kontejnerů
- Podpora Secure Boot
- Plnohodnotná integrace do XDR

Podporované operační systémy pro instalaci agenta (v některých případech s využitím starší verze agenta a omezeným počtem funkcí):

- Windows 2000, Windows XP a novější
- Windows Server 2003 SP1 a novější
- Linux:
 - o Red Hat 5 a novější
 - o Ubuntu 10 a novější
 - o CentOS 5 a novější
 - o Debian 6 a novější
 - o SUSE Linux 10 a novější
- Solaris 10 a novější
- Ochrana pomocí agenta ve virtuálního prostředí bez ohledu na technologii virtualizace

Možnost nasazení bez agenta pomocí VMware NSX a virtuální appliance. Při využití NSX Advanced nebo NSX Enterprise musí být podporovány tyto moduly:

- Antimalware (Windows)
- Integrity monitoring (Windows)
- Firewall
- Intrusion Prevention
- Webová reputace

Antimalware

- Antimalware sken v reálném čase (RealTime scan)
- Smart Scan pro optimalizaci vytížení CPU při detekci signatur
- Strojové učení využívající databázi v cloudu
- Detekce škodlivého chování (Behavior monitoring)
- Ochrana proti ransomware
- Ochrana před spyware a grayware
- Sken procesů běžících v operační paměti, detekce škodlivé aktivity
- Možnost nastavení výjimek:
 - o Adresář

- Soubor
- Přípona souboru
- Proces

Kontrola webových stránek (Web Reputation)

- Blokace webových stránek na základě hodnocení výrobce nabízeného řešení
- Možnost blokace na základě kategorií:
 - Nebezpečné
 - Vysoce podezřelé
 - Podezřelé
 - Neotestované

Kontrola aplikací (Application Control)

- K dispozici dva módy:
 - Blokace všech nových aplikací, pokud nejsou schváleny
 - Povolení všech aplikací, pokud nejsou zakázány
- Mód údržby (Maintenance mode) pro dočasné povolení spuštění aplikací při plánovaných změnách na serveru
- Notifikace v případě spuštění zakázané aplikace
- Možnost povolení aplikace z administračního rozhraní na základě vygenerované notifikace
- Možnost nastavení výjimek na základě certifikátu

Sledování integrity

- Sledování změn v pravidelných intervalech (naplánovaná úloha) nebo v reálném čase
- Možnost automatického přebírání pravidel z automatických naplánovaných skenů, které aktualizují doporučenou politiku pro sledování integrity
- Podpora pro definici vlastních pravidel pro sledování změn v systému:
 - Změna v registrech
 - Obsah souboru
 - Atributy souboru
 - Definice také pomocí XML
 - Nastavení závažnosti
- Možnost úpravy nastavení vytížení CPU při skenování integrity systému
 - Vysoké
 - Střední (vkládání pauzy v procesu skenování pro snížení zátěže CPU)
 - Nízké (vkládání pauzy v procesu skenování pro snížení zátěže CPU)

Sledování logů

- Možnost automatického přebírání pravidel z automatických naplánovaných skenů, která aktualizují politiku pro sledování logů
- Přebírá logy z různých zdrojů (Windows events, syslog, IIS, Apache, ...) a ukládá v jednotném formátování do vlastní databáze
- Možnost přeposílání logů do externího syslog serveru (SIEMu)
- Auto-tagging umožní např. označit všechny logy, kdy se někdo neúspěšně přihlásil k serveru a odmazat automaticky ty logy, které obsahují „oprávněného“ uživatele, a zůstanou logy neoprávněných „útočníků“
- Události lze dát váhu podle modulu a „důležitosti“ serveru/desktopu
- Možnost definice vlastních pravidel a notifikací pro sledování logů:
 - Detekce definovaných řetězců v logu
 - Využití regulárních výrazů

- Definice závažnosti logů
- Monitoring událostí z Windows event logu

Firewall

- Filtrování příchozího a odchozího provozu pomocí stavového firewallu na úrovni síťové karty
- Dostupné akce na definovaná spojení:
 - Bypass (nejsou aplikována žádná další pravidla, neprobíhá inspekce v rámci IPS)
 - Log Only (pouze loguje)
 - Force Allow (povoleno s nejvyšší prioritou, má přednost pravidly Deny)
 - Deny (zakázáno)
 - Allow (povoleno)
- Možnost definice priority pro jednotlivá pravidla (která následně mají přednost před jejich pořadím v rámci konfigurace politiky) v rozmezí 0 (nejnižší) až 4 (nejvyšší)
- Firewall dostupný ve dvou módech:
 - Tap mód – do síťové komunikace není nijak zasahováno, firewall funguje pouze v detekčním/logovacím módu, vhodné pro testování
 - Inline mód – síťová komunikace prochází přes definovaná pravidla a na provoz jsou aplikovány definované akce na základě politiky a nastavených pravidel
- Podpora nastavení pro „fail close/fail open“ – nastavení chování firewallu v případě chyby, systémového problému nebo problému při kontrole síťových paketů
- Podpora restriktivního (co není povoleno, je zakázáno) i permisivního módu (co není zakázáno, je povoleno)
- Speciální pravidlo bypass, které znamená výjimku jak na Firewall modulu, tak na modulu IPS pro optimalizaci vytížení při inspekci.
- Podpora detekce skenování (získávání informací před útokem):
 - Detekce otisku operačního systému
 - Detekce skenování portů
 - Detekce TCP null skenu
 - Detekce TCP SYNFIN skenu
 - Detekce TCP XMAS skenu

Ochrana před síťovými útoky (Intrusion Prevention)

- Systém pro detekci a blokování útoků a exploitace na úrovni síťové karty
- Virtuální záplatování (Virtual Patching) – instalace ochrany na síťové úrovni na zranitelnosti vyskytující se v operačním systému a nainstalovaných aplikacích
- Automatický sken zranitelností, který je součástí agenta a který prohledá operační systém, detekuje verzi operačního systému, detekuje instalované aktualizace, detekuje verze nainstalovaných programů a jejich verzí, a doporučí relevantní pravidla pro IPS (takzvané virtuální záplaty)
- Možnost automatického přebírání pravidel z automatických naplánovaných skenů a automatická aktualizace politiky dle aktuálního stavu operačního systému a nainstalovaných aplikací - automatický virtuální patching
- Možnost fungování v detekčním módu nebo preventivním módu
- Podpora SSL/TLS inspekce
- Podpora TLS inspekce pomocí kernel hooking bez nahrávání certifikátu, bez podvrhování certifikátu, včetně podpory PFS.
- Možnost využívání tagů na síťových rozhraních
- Možnost přiřadit pravidla konkrétním síťovým rozhraním

- Ochrana před SQL injection
- Ochrana proti technikám obcházejících IPS, například:
 - o Neplatná TCP časová razítka
 - o Fragmentované pakety
 - o Neplatné kontrolní součty
 - o Data obsažená v TCP SYN
 - o Neplatné flagy TCP spojení
 - o Duplikace dat při navazování spojení

Activity Monitoring

- Modul, který sbírá veškeré údaje ze serveru a ty zasílá do XDR konzole, kde je lze analyzovat

Kvalita nabízeného řešení:

- o Nabízené řešení, resp. jeho výrobce, musí být v mezinárodně platném benchmarkovém reportu pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“, přičemž předmětem benchmarkového reportu musí být EDR (Endpoint Detection and Response) technologie kybernetické bezpečnosti a benchmark musí obsahovat posouzení minimálně TOP10 celosvětových výrobců. (např. Gartner Magic Quadrant for Endpoint Protection Platforms)

XDR systém

Technické požadavky na XDR

Obecné vlastnosti:

- Centrální jednotná konzole pro vyšetřování incidentů, Security operation center (SOC)
- Platforma celého řešení umístěná v cloudovém prostředí výrobce řešení
- Podpora plnohodnotné integrace produktů EDR požadovaných výše
- Podpora plnohodnotné integrace rovněž i produktů třetích stran
- Podpora pro napojení produktů třetích stran pomocí otevřeného API

Další klíčové vlastnosti XDR:

- Možnost retence logů 30 až 365 dní
- Instalovaný XDR agent dokáže detekovat zranitelnosti na systému, kde je nainstalovaný
- Obsahuje Sandbox SaaS s možností manuálního nahrání vzorků
- Podpora instalace samostatného XDR agenta pro Windows, Linux, MacOS
- Obsahuje detekční modely spravované výrobcem nabízeného řešení XDR, na základě, kterých probíhá korelace XDR dat, s možností nastavení výjimek pro dané detekční modely
- Obsahuje specializované IOC (indicators-of-compromise) feedy spravované výrobcem nabízeného řešení XDR, které monitorují známé malware kampaně
- Obsahuje specializované IOC feedy poskytovatelů třetích stran
- Možnost zadávat ručně IOC objekty a další Threat Intelligence, které lze následně používat.

Podpora:

- o STIX
- o CSV
- o TAXII
- o MISP
- Přehledná vizualizace XDR detekce / incidentu, provázanost objektů mezi sebou a detailní informace o každém objektu
- Přehledná vizualizace EDR dat z koncového zařízení či serveru (viz požadavky výše), kde je vidět, jak byl proces spuštěn, jaké prováděl změny na filesystému, jaká probíhala síťová komunikace a tak dále
- Jednotlivé detekce automaticky korelují detekce/alerty do komplexních incidentů na základě společných objektů (například IP adresy, endpointy, domény, shodné soubory apod.)
- Široké možnosti response akcí:
 - o Izolace agenta od sítě
 - o Odeslání souboru do Sandboxu
 - o Stažení souboru z agenta
 - o Přihlášení na příkazovou řádku agenta (následně možnost ukončit proces, prohlédnout registry, soubory apod.)
 - o Spuštění skriptu (powershell/bash)
 - o Blokace objektu (soubor, hash, IP adresa, doména)
 - o Blokace e-mailu odesílatele
 - o Přesun e-mailu do karantény nebo smazání emailu
- Veškeré response akce jsou automaticky auditovány
- Blokované objekty je možné automaticky roz distribuovat na připojené ochranné produkty, které toto umožňují
- Možnost exportu provedeného vyšetřování do souboru

- Logy automaticky obohaceny o informace dle MITRE, doplnění logů o MITRE techniky a taktiky
- Možnost konfigurace přístupu do Administrační konzole XDR na základě rolí a přidělení konkrétních práv
- Možnost rozšíření XDR o další licencované funkcionality typu Managed XDR (není předmětem poptávky v rámci této veřejné zakázky, nicméně do budoucna musí být tyto funkcionality v řešení k dispozici po jejich zalicencování nebo nákupu):
 - o Kontrolu logů a analýzu alertů provádí specializovaný tým vyškolených expertů výrobce
 - o Zasílání pravidelných reportů
 - o Filtrace False positives
 - o Monitoring 24/7
 - o Provádění a analýza „Root Casue“
 - o Poskytnutí doporučeného postupu jak se s danou hrozbou nebo útokem vyrovnat
- Integrace s případnými interními (on-premise) systémy musí probíhat skrze Service Gateway, která zprostředkovává komunikaci s řešením XDR bez potřeby nutnosti otevření portů z internetu.

Požadavky na aplikační konzoli XDR:

- Dashboard informace a přehled aktuálních informací za posledních 7 dní
 - Souhrn používaných cloud aplikací napříč zařízeními
 - TOP 10 rizikových aplikací
 - TOP 10 rizikových uživatelů
 - TOP 10 rizikových zařízení
 - TOP 10 nepoužívanějších aplikací dle kategorií
 - Používané aplikace dle kategorií (graf)
 - Historie detekcí za posledních 7 dní
 - Přehled zařízení s nejvíce detekovanými útočnými technikami dle MITRE
 - Přehled o aktivitě koncových zařízení
- Předpřipravené skeny/detekce od výrobce nabízeného řešení XDR připravené na konkrétní kampaně nebo aktuální zranitelnosti např.:
 - Samba Vulnerability (CVE-2021-44142)
 - Log4Shell Vulnerability
 - Risk assessment
 - Cloud Maibox Assessment (Microsoft 365)
- Možnost napojení na externí Threat Intelligence feedy
- Nastavení vlastních IOC
- Distribuce a sdílení podezřelých/blokovaných objektů
- Sandbox analýza
- TAXII
- MISP
- Detailní přehled o:
 - o Uživatelích
 - o Zařízeních
 - o IP adresách
 - o Používaných aplikacích
- Aplikace zobrazující výsledky vyšetřování, detekce a varování. Slouží zejména k:

- Vygenerování analýzy příčiny problému (Execution Profile)
- Zobrazení profilu daného objektu (jakým způsobem byl spuštěn, kam se dotazoval, co spustil, atd...)
- Identifikace dopadu, informace o výskytu dané detekce v síti
- Zobrazení detailních informací o objektu, například parametry příkazu z příkazové řádky
- Možnost provedení akce pro EDR:
 - Stažení souboru z koncové stanice (například k další analýze)
 - Přidat daný objekt na seznam blokových
 - Odebrat objekt z blokových
 - Izolovat koncové zařízení (Endpoint)
 - Obnovit spojení s izolovaným zařízením
 - Připojení se příkazový řádek stanice
- Možnost označení detekcí příznakem pro evidenci vyšetřování (probíhá vyšetřování, uzavřeno, false positive...)
- Veškeré logy, které lze napárovat na konkrétní MITRE techniku/taktiku
- Možnost filtrování na základě endpointu, času, techniky, taktiky
- Logy jsou interaktivní a mohou sloužit jako start pro další hledání nebo generování vizualizace (Execution profile)
- Aplikace pro vyhledávání informací a objektů v databázi všech XDR logů
 - Vyhledávání podle IOC
 - Lze provádět vyhledávání objektů v historických datech na základě:
 - Doména
 - EndpointID
 - Hostname
 - IP adresa (v4 a v6)
 - Cesta k souboru na disku
 - MD5, SHA1, SHA2 souboru
 - Název souboru
 - Port
 - Cesta k procesu
 - Název Procesu
 - Klíč v registru
 - Hodnota v registru
 - Data v registru
 - Taktika dle MITRE
 - Technika dle MITRE
 - URL
 - Uživatelský účet
 - Příkaz z příkazové řádky
 - Dotaz pro vyhledávání lze uložit pro příště
 - Dotaz pro vyhledávání lze uložit na Watchlist a XDR následně automaticky provádí vyhledávání
- Aplikace s přehledem všech detekčních modelů, které korelují posbíraná data a provádějí jejich vyhodnocení.
 - Možnost aktivace/deaktivace jednotlivých modelů
 - Konfigurace rizika pro jednotlivé modely

- Detekční modely jsou předpřipravené a pravidelně doplňované přímo od výrobce nabízeného řešení XDR
- Aplikace pro přehled všech provedených akcí
 - Evidence všech provedených akcí
 - Možnost provádění auditu historie vyšetřování

Podpora provozu

Technické požadavky na podporu provozu

Zadavatel požaduje, aby účastník po poskytnutí licencí pro EDR a XDR řešení zahájil poskytování konzultační a technická podpory provozu pro dodané a implementované řešení s následujícími parametry:

- Měsíční alokace zdrojů: 1 člověkodenní za měsíc
- Dostupnost podpory:
 - Web-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
 - Email-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
 - Telefonický helpdesk pro konzultace v režimu 8x5
 - Veškerá konzultační a technická podpora bude poskytována v režimu 8x5, tj. v pracovní dny v běžnou pracovní dobu

Podpora implementace

Technické požadavky na podporu implementace

Zadavatel požaduje, aby účastník v implementační fázi zajistil pro potřeby projektu pracovníka pro roli „Implementačního specialisty“, který bude provádět faktickou implementaci management konzolí nabízeného řešení a poskytovat konzultační aktivity a poradenství pro pracovníky zadavatele ve vztahu k nasazení bezpečnostních agentů na koncové stanice a servery.

Implementační fáze bude trvat maximálně 3 měsíce od poskytnutí licencí pro EDR a XDR systémy.

Maximální rozsah implementační podpory představuje v souhrnu 10 člověkodenní využitelných během uvedených 3 měsíců trvání implementace.

Příloha č. 1B

Technická specifikace plnění – popis účastníka

EDR / XDR licence

Kód (SKU)	Položka	Ks
EDR pro koncové stanice		
OS01136773	Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, New, Normal, 101-250 User License,12 months	150
OS01136917	Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, Renew, Normal, 101-250 User License,12 months	150
OS01137205	Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, Renew, Normal, 101-250 User License,36 months	150
EDR pro servery		
CX01177566	Trend Micro Cloud One - Workload Security with XDR, New, Government, 1-50 License,12 months	29
CX01177710	Trend Micro Cloud One - Workload Security with XDR, Renew, Government, 1-50 License,12 months	29
CX01177998	Trend Micro Cloud One - Workload Security with XDR, Renew, Government, 1-50 License,36 months	29
XDR		
VO01158935	Trend Micro Vision One Credits, Government, License, 3000 credits for 5 years	1

Podpora provozu

Po poskytnutí licencí pro EDR a XDR řešení bude zahájeno poskytování konzultační a technická podpory provozu pro dodané a implementované řešení s následujícími parametry:

- Měsíční alokace zdrojů: 1 člověkoden za měsíc
- Dostupnost podpory:
 - o Web-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
 - o Email-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
 - o Telefonický helpdesk pro konzultace v režimu 8x5
 - o Veškerá konzultační a technická podpora bude poskytována v režimu 8x5, tj. v pracovní dny v běžnou pracovní dobu

Kontakty na dodavatele:

- Web based helpdesk: support.altepro.cz
- Telefonická podpora: +420 840 11 22 33
- E-mailová podpora: support@altepro.cz

Podpora implementace

V implementační fázi bude zajištěn pro potřeby projektu pracovník pro roli „Implementačního specialisty“, který bude provádět faktickou implementaci management konzolí nabízeného řešení a poskytovat konzultační aktivity a poradenství pro pracovníky zadavatele ve vztahu k nasazení bezpečnostních agentů na koncové stanice a servery.

Implementační fáze bude trvat maximálně 3 měsíce od poskytnutí licencí pro EDR a XDR systémy.

Maximální rozsah implementační podpory představuje v souhrnu 10 člověkodnů využitelných během uvedených 3 měsíců trvání implementace.

PŘÍLOHA Č. 2 SMLOUVY

Výpočet nabídkové ceny

Podlimitní veřejná zakázka, zjednodušené podlimitní řízení

"NCO NZO Brno – Systémová ochrana 2022"

ID zakázky: VZ0149985

Dílní hodnotící kritéria	Název produktu	Jednotkové ceny		Počty jednotek	Jednotky	Celkové ceny	
		Cena v Kč bez DPH	Cena v Kč vč. DPH			Cena v Kč bez DPH	Cena v Kč vč. DPH
EDR – ochrana koncových stanic před kybernetickými hrozbami na 5 let (licence na 1 koncovou stanicí)	Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, New, Normal, 101-250 User License, 12 months (OS01136773) + Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, Renew, Normal, 101-250 User License, 12 months (OS01136917) + Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central, Renew, Normal, 101-250 User License, 36 months (OS01137205)	4 157,00	5 029,97	150	ks	623 550,00	754 495,50
EDR – ochrana serverů před kybernetickými hrozbami na 5 let (licence na 1 server)	Trend Micro Cloud One - Workload Security with XDR, New, Government, 1-50 License, 12 months (CX01177566) + Trend Micro Cloud One - Workload Security with XDR, Renew, Government, 1-50 License, 12 months (CX01177710) + Trend Micro Cloud One - Workload Security with XDR, Renew, Government, 1-50 License, 36 months (CX01177998)	31 520,00	38 139,20	29	ks	914 080,00	1 106 036,80
XDR – rozšíření funkcionality EDR (licence pro celé řešení)	Trend Micro Cloud One - Workload Security with XDR, New, Government, 1-50 License, 12 months (CX01177566)	315 195,00	381 385,95	1	komplet	315 195,00	381 385,95
Podpora provozu (1 člověkoden měsíčně od poskytnutí licencí pro EDR a XDR systémy)	Podpora provozu po dobu 60 měsíců v rozsahu 1 MD měsíčně (cena za 1 měsíc)	5 000,00	6 050,00	60	měsíců	300 000,00	363 000,00
Podpora implementace (čerpatelné během 3 měsíců od poskytnutí licencí pro EDR a XDR systémy)	Podpora implementace po dobu 3 měsíců v rozsahu 10 MD (cena za 1 MD)	20 000,00	24 200,00	10	člověkodů	200 000,00	242 000,00
Celková cena						2 352 825,00	2 846 918,25

* Vyplňte pouze žlutě označené pole

Datum:

Účastník(Firma): ALTEPRO solutions a.s.

Jméno a podpis oprávněné osoby: Martin Vitek, člen představenstva

ZADÁVACÍ DOKUMENTACE K PODLIMITNÍ VEŘEJNÉ ZAKÁZCE

Veřejná zakázka zadávaná podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, s ohledem na znění § 53 a ve spojení s § 6 tohoto zákona.

1. NÁZEV PODLIMITNÍ VEŘEJNÉ ZAKÁZKY

Název veřejné zakázky:	NCO NZO Brno – Systémová ochrana 2022
ID zakázky (Tender arena)	VZ0149985

2. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE

Obchodní firma nebo název / obchodní firma nebo jméno a příjmení:	Národní centrum ošetrovatelství a nelékařských zdravotnických oborů
Sídlo / místo podnikání / místo trvalého pobytu (příp. doručovací adresa):	Vinařská 965/6, Brno, PSČ 603 00
IČ:	00023850
Osoba oprávněná jednat jménem či za zadavatele:	PhDr. Mgr. Michaela Hofštetrová Knotková, ředitelka

3. IDENTIFIKAČNÍ ÚDAJE OSOBY ZASTUPUJÍCÍ ZADAVATELE

Obchodní firma nebo název / obchodní firma nebo jméno a příjmení:	Národní centrum ošetrovatelství a nelékařských zdravotnických oborů
Sídlo / místo podnikání / místo trvalého pobytu (příp. doručovací adresa):	Vinařská 965/6, Brno, PSČ 603 00
IČ:	00023850
Osoba oprávněná za osobu zastupující zadavatele jednat:	Ing. Jaroslav Kratochvíl, náměstek ředitele pro úsek ekonomický a technický
Kontaktní osoba:	Mgr. Vojtěch Pilarš
Telefon, fax, e-mail:	+420 543 559 254, pilar@nconzo.cz

4. VYMEZENÍ PŘEDMĚTU VEŘEJNÉ ZAKÁZKY A PODMÍNEK PLNĚNÍ

Druh veřejné zakázky: Veřejná zakázka na služby a dodávky
Kód a název NÍPEZ: 48761000-0 Balík antivirových programů

4.1. Předmět plnění veřejné zakázky:

Předmětem veřejné zakázky je zajištění dodávky softwarového řešení nástroje pro ochranu před škodlivých kódem ve smyslu §21 dle vyhlášky č. 82/2018 Sb. resp. §5 odst. 3) 181/2014 Sb. e) nástroj pro ochranu před škodlivých kódem. Součástí plnění je zajištění všech činností souvisejících se zajištěním požadovaných služeb a dodávky předmětu zakázky.

Specifikace a technické požadavky jsou uvedeny v příloze č. 6 Technická specifikace předmětu plnění.

Zadávací dokumentace je účastníkům k dispozici na profilu zadavatele na adrese: <https://www.tenderarena.cz/profil/detail.jsf?identifikator=nconzo>.

Kontakt na osobu oprávněnou jednat ve věci poskytnutí technických informací: Mgr. Vojtěch Pilar, tel. 543 559 254, e-mail pilar@nconzo.cz.

4.2. Místo plnění:

Místem plnění je sídlo zadavatele: Vinařská 965/6, 603 00 Brno.

4.3. Obecná ustanovení:

Vázanost účastníka nabídkou do 31. 12. 2022

V případě, že zadavatel vyžaduje v nabídce podepsaný dokument, musí být tento dokument podepsán osobou oprávněnou jednat za účastníka. Pokud jedná jménem účastníka či za účastníka osoba odlišná od osoby oprávněné za účastníka jednat, musí být součástí nabídky plná moc opravňující tuto osobu k příslušnému jednání. Tato plná moc musí být v originále nebo v úředně ověřené kopii součástí nabídky.

Účastník nemá právo na úhradu nákladů spojených s účastí na této zakázce.

Zadavatel si vyhrazuje právo na změnu, upřesnění nebo doplnění zadávacích podmínek, a to na základě žádostí zájemců o vyjasnění zadání, nebo z vlastního podnětu. Tuto změnu obsahu zadání zadavatel oznámí všem účastníkům, kteří byli k podání nabídky vyzváni. Změna bude provedena písemnou formou nejméně 4 pracovní dny před uplynutím lhůty pro podání nabídek.

Zadavatel si vyhrazuje zveřejnit na svém profilu zadavatele informace o výsledku řízení, o vyloučení účastníka a o zrušení zakázky.

Zadavatel si vyhrazuje právo zrušit zadání této zakázky.

5. OBCHODNÍ PODMÍNKY

Zadavatel vymezuje obchodní podmínky v zadávací dokumentaci. Tyto obchodní podmínky a technická specifikace předmětu veřejné zakázky budou obsaženy v návrhu smlouvy, kterou předloží účastník jako součást nabídky.

Předmět plnění veřejné zakázky viz odstavec 4.1. této zadávací dokumentace.

V následující části zadávací dokumentace jsou některé obchodní podmínky blíže vymezeny.

5.1. PLATEBNÍ PODMÍNKY

Pro vzájemný platební styk bude použito daňových dokladů (faktur) vystavených dodavatelem. Splatnost faktury je stanovena na 21 dnů ode dne doručení objednateli. Splatností se rozumí odepsání finančních prostředků z účtu objednatele.

Objednatel souhlasí se zasíláním elektronických daňových dokladů od zhotovitele ve formátu *.pdf, odpovídajících příslušným ustanovením zákona o DPH.

Fakturace bude prováděna na základě skutečně odebraných služeb za uplynulé období.

Daňový doklad (faktura) musí obsahovat veškeré náležitosti dle platné legislativy.

Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.

5.2. DODACÍ PODMÍNKY

Dodavatel po dobu trvání této smlouvy v obvyklé pracovní době zajistí následující:

- technickou podporu implementace dodávaného řešení (specifikace v příloze č. 6),
- technickou podporu provozu (specifikace v příloze č. 6),

Objednatel si vyhrazuje právo od smlouvy odstoupit bez uvedení důvodu s maximálně tříměsíční výpovědní lhůtou bez finančního vyrovnání.

5.3. SANKČNÍ PODMÍNKY

Smluvní strany sjednají smluvní pokutu ve výši 0,05 % z dlužné částky za každý započatý den prodlení se zaplacením daňového dokladu.

5.4. NÁVRH SMLOUVY

Účastník předloží vlastní návrh smlouvy, který bude splňovat následující parametry:

- 1. etapa projektu: Poskytnutí licencí
 - o Licence budou poskytnuty nejpozději k datu 21.11.2022 a budou platné na období 5 let
 - o Poskytnutí licencí skrze licenční portál výrobce je prvním fakturačním milníkem
- 2. etapa projektu: Podpora provozu
 - o Měsíční rozsah této podpory představuje objem prací na úrovni 1 člověkodne v měsíci
 - o Fakturace bude probíhat na měsíční bázi vždy za předchozí měsíc
- 3. etapa projektu: Podpora implementace v prostředí zákazníka
 - o Poskytnutí konzultační aktivity a poradenství pro pracovníky zadavatele ve vztahu k nasazení bezpečnostních agentů na koncové stanice a servery bude probíhat po dobu prvních 3 měsíců po poskytnutí licencí
 - o Rozsah podpory implementace: maximálně 10 člověkodní
 - o Fakturace proběhne po protokolárním dokončení implementace, či po vyčerpání celkového rozsahu implementace

6. POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

Nabídková cena bude vyčíslena stanovením jednotkových cen za předmět plnění a vynásobením předpokládaným objemem za dobu trvání smlouvy. Účastník provede výpočet nabídkové ceny na přiloženém formuláři ve formátu *.xlsx – příloha č. 3 zadávací dokumentace. Účastník použije elektronickou podobu tohoto formuláře zveřejněnou v dokumentech zakázky na profilu zadavatele (viz odstavec 4.1). Suma těchto hodnot je nabídkovou cenou, kterou účastník uvede ve formuláři „Krycí list nabídky (příloha č. 1 zadávací dokumentace). Pro posouzení nabídek je rozhodující cena bez DPH.

Účastník ručí za správné načítání a sčítání v nabídce odevzdaných tabulkách. Chyba v matematických operacích může být důvodem k vyloučení. V případě jakéhokoli nesouladu mezi nabídkou účastníka a tabulkami předloženými zadavatelem, může hodnotící komise vyřadit nabídku z dalšího posuzování.

Další požadavky na cenu:

- Nabídková cena bude uvedena v CZK, celou částkou za celé plnění veřejné zakázky.

- Nabídková cena bude uvedena v členění: nabídková cena bez daně z přidané hodnoty (DPH), samostatně DPH včetně uvedení sazby DPH a nabídková cena včetně DPH.
- Nabídková cena bude zahrnovat veškeré náklady účastníka spojené s plněním celého předmětu veřejné zakázky.
- Účastník je povinen v nabídce uvést jednotkové ceny za požadované druhy položek.

Účastníkem stanovená nabídková cena je cenou nejvýše přípustnou a nepřekročitelnou po celou dobu plnění předmětu veřejné zakázky se započtením veškerých nákladů, rizik, zisku a finančních vlivů (např. inflace) po celou dobu realizace zakázky v souladu se zadávacími podmínkami uvedenými v této zadávací dokumentaci. Ceny budou zahrnovat veškeré náklady uchazeče související s realizací předmětu veřejné zakázky.

Krycí list nabídky bude podepsán osobou oprávněnou jednat jménem či za účastníka. Pokud jedná jménem či za účastníka jiná osoba odlišná od osoby oprávněné jednat, musí být součástí nabídky plná moc opravňující tuto osobu k jednání. Tato plná moc musí být předložena v originále nebo v úředně ověřené kopii.

7. JINÉ POŽADAVKY ZADAVATELE NA PLNĚNÍ VEŘEJNÉ ZAKÁZKY

7.1. Účastník je povinen být pojištěn po celou dobu plnění předmětu této veřejné zakázky na odpovědnost za škodu způsobenou dodavatelem třetí osobě v minimálním rozsahu 2 mil. Kč.

7.2. Nezadání zakázky

Účastník doloží do nabídky prohlášení o tom, že zadávacího řízení se neúčastní obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a to ani jako poddodavatel, prostřednictvím kterého dodavatel prokazuje kvalifikaci.

Dále účastník doloží do nabídky prohlášení o tom, že se dodavatele ani jeho poddodavatele netýkají mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. V případě, že na dodavatele anebo poddodavatele sankce dopadají, uveďte jaké.

8. POŽADAVKY NA KVALIFIKACI

8.1. Základní způsobilost účastníka.

Účastník v nabídce k prokázání základní způsobilosti předloží čestné prohlášení o své základní způsobilosti. K tomuto účelu použije přílohu č. 2 zadávací dokumentace „Čestné prohlášení o splnění základní způsobilosti účastníka“, podepsanou osobou oprávněnou jednat jménem či za účastníka. Pokud jedná jménem či za účastníka jiná osoba odlišná od osoby oprávněné jednat, musí být součástí nabídky plná moc opravňující tuto osobu k jednání. Tato plná moc musí být předložena v originále nebo v úředně ověřené kopii.

8.2. Profesní způsobilost účastníka.

Účastník v nabídce k prokázání profesní způsobilosti předloží:

- kopii výpisu z obchodního rejstříku, pokud je v něm zapsán, či výpis z jiné obdobné evidence, pokud v ní má být účastník podle právních předpisů zapsán.
- kopii dokladu o oprávnění k podnikání podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu veřejné zakázky, zejména dokladu prokazující příslušné živnostenské oprávnění či licenci.

Uvedené doklady předkládá v prosté kopii.

8.3. Technická kvalifikace.

Seznam významných zakázek

Účastník prokáže splnění kritéria čestným prohlášením, které bude obsahovat seznam významných služeb realizovaných účastníkem v posledních 3 letech, každá z nich spočívající v dodávce licencí EDR systémů s počtem uživatelských licencí minimálně 100 ks a v hodnotě minimálně 300 000 Kč bez DPH.

Účastník splní kritérium významných zakázek, pokud v daném období realizoval minimálně dvě (2) takové zakázky a alespoň jedna ze seznamu významných zakázek pokrývá i ochranu serverů před kybernetickými bezpečnostními událostmi v počtu minimálně 50 ks licencí.

Účastník prokáže toto kritérium předložením seznamu dodávek s údaji:

- a. Objednatel
- b. Stručný popis předmětu plnění (informace o počtu a typu licencí)
- c. Hodnota (tj. částka za dodávku)
- d. Období realizace
- e. Kontakt na osobu, u které může být reference ověřena

Odborná kvalifikace uchazeče

Účastník prokáže splnění kritéria odborná kvalifikace uchazeče předložením osvědčením o odborné kvalifikace vztahující se k požadovaným dodávkám a službám. Účastník prokáže splnění tohoto kritéria, pokud z předložených dokumentů (např. certifikátu vydaného výrobcem nabízeného řešení nebo potvrzení vystaveného zastoupením výrobce nabízeného řešení pro Českou republiku) bude vyplývat, že dodavatel může poskytovat na území České republiky prodejní, servisní a jiné služby týkající se produktů výrobce, které jsou předmětem nabídky.

Technický tým

Účastník prokáže splnění kritéria technický tým předložením seznamu techniků, kteří se budou podílet na plnění předmětu veřejné zakázky, a to včetně doložení jejich odborné kvalifikace vtaující se k požadovaným službám. Účastník předloží, že disponuje alespoň následujícím technickým týmem:

- a. Projektový manažer
 - Platná certifikace pro oblast IT service managementu na úrovni ITIL v3 nebo vyšší či obdobnou metodiku
 - Platnou certifikaci pro projektového manažera na úrovni Prince2 nebo IPMA C nebo obdobnou či vyšší
- b. Implementační specialista
 - Platnou certifikaci výrobce nabízeného řešení na úrovni „certified professional“ nebo vyšší

Účastník, jehož nabídka bude vybrána jako nejvhodnější, je povinen předložit zadavateli k ověření originály nebo úředně ověřené kopie dokladů prokazujících splnění kritéria technické kvalifikace, a to do dne uzavření smlouvy na předmět této veřejné zakázky.

9. ZPŮSOB HODNOCENÍ NABÍDEK

Kritériem hodnocení je ekonomická výhodnost nabídky. Zadavatel stanovuje hodnotícím kritériem nabídkovou cenu s váhou 100%. Toto kritérium je minimalizační.

Účastník není oprávněn podmínit jím navrhované údaje, které jsou předmětem hodnocení, další podmínkou. Podmínění nebo uvedení několika rozdílných hodnot je důvodem pro vyřazení nabídky a vyloučení účastníka ze zadávacího řízení. Obdobně bude zadavatel postupovat v případě, že dojde k uvedení hodnoty, která je předmětem hodnocení, v jiné veličině či formě, než zadavatel stanovil.

9.1. Způsob hodnocení nabídek:

Pro hodnocení nabídek zadavatel použije bodovací stupnici v rozsahu 0 až 100. Každé jednotlivé nabídce je dle hodnotícího kritéria přidělena bodová hodnota, která odráží úspěšnost předmětné nabídky v rámci kritéria.

Pro hodnotící kritérium „Nabídková cena“, získá hodnocená nabídka bodovou hodnotu, která vznikne násobkem 100 a poměru hodnoty nejhodnější nabídky k hodnocené nabídce v rámci hodnotícího kritéria, zaokrouhlenou na jedno desetinné místo.

Nabídka s nejvyšším počtem bodů bude vybrána jako nejhodnější.

10. PODMÍNKY A POŽADAVKY PRO ZPRACOVÁNÍ NABÍDKY

- 10.1. Nabídka bude předložena v originále v písemné formě a dále rovněž v elektronické formě na vhodném médiu (USB Flash Disk), v českém jazyce.
- 10.2. Nabídka bude předložena ve formě popisu souladu nabízeného řešení s požadavky zadavatele, odkazem na technickou specifikaci výrobce, příložením datasheetu, či jiným obdobným způsobem, ze kterého bude zřejmé splnění požadavků zadavatele.
- 10.3. Nabídka nebude obsahovat přepisy a opravy, které by mohly zadavatele uvést v omyl.
- 10.4. Všechny listy nabídky včetně příloh budou řádně očíslovány vzestupnou číselnou řadou a nabídka bude zajištěna proti neoprávněné manipulaci.
- 10.5. Účastník použije pořadí dokumentů specifikované v následujících bodech těchto pokynů pro zpracování nabídky:
 - 10.5.1. **Krycí list nabídky.** Účastník vyplní formulář, který je součástí zadávací dokumentace. Krycí list nabídky bude podepsán osobou oprávněnou jednat jménem či za účastníka. Pokud jedná jménem či za účastníka jiná osoba odlišná od osoby oprávněné jednat, musí být součástí nabídky plná moc opravňující tuto osobu k jednání. Tato plná moc musí být předložena v originále nebo v úředně ověřené kopii.
 - 10.5.2. **Obsah nabídky.** Nabídka bude opatřena obsahem s uvedením čísel listů u jednotlivých oddílů (kapitol).
 - 10.5.3. **Prohlášení účastníka** dle odst. 7.2 zadávací dokumentace
 - 10.5.4. **Doklady a dokumenty k prokázání splnění kvalifikace.**

Čestné prohlášení o splnění základní způsobilosti účastníka podepsané osobou oprávněnou jednat jménem či za účastníka, dle odst. 8. 1. zadávací dokumentace.

Doklady o splnění profesní způsobilosti účastníka v prosté kopii, dle odst. 8. 2. zadávací dokumentace.

Doklady o splnění kritérií technické kvalifikace dle odst. 8. 3. zadávací dokumentace.

10.5.5. Hodnoty hodnotících kritérií.

V této části účastník uvede položkový rozpočet ceny za celý předmět plnění. K výpočtu nabídkové ceny účastník použije formulář, který je přílohou č. 3 této zadávací dokumentace, podepsaný osobou oprávněnou jednat za účastníka.

10.5.6. Podepsaný návrh Smlouvy na předmět zakázky.

Účastník v nabídce předloží návrh smlouvy, podepsaný osobou oprávněnou jednat jménem či za účastníka. Pokud jedná jménem či za účastníka jiná osoba odlišná od osoby oprávněné jednat, musí být součástí návrhu Smlouvy plná moc opravňující tuto osobu k jednání. Tato plná moc musí být předložena v originále nebo v úředně ověřené kopii.

Návrh smlouvy musí v plném rozsahu respektovat obchodní podmínky stanovené v oddíle 5 této zadávací dokumentace. V případě nesplnění této podmínky může zadavatel účastníka vyloučit.

10.5.7. Ostatní doklady a dokumenty požadované zadavatelem.

Souhlas se zveřejněním budoucího smluvního vztahu, zpracovaný na vzoru, který je přílohou č. 4 zadávací dokumentace. Souhlas bude podepsán osobou oprávněnou jednat jménem či za účastníka.

Čestné prohlášení o počtu listů nabídky zpracované na vzoru, který je přílohou č. 5 zadávací dokumentace. Čestné prohlášení bude podepsáno osobou oprávněnou jednat jménem či za účastníka.

11. DODATEČNÉ INFORMACE K ZADÁVACÍ DOKUMENTACI

Žádost o dodatečné informace k zadávací dokumentaci je možno doručit písemně (e-mail) nejpozději do pěti pracovních dnů před koncem lhůty pro podání nabídek, kontaktní osoba: Mgr. Vojtěch Pilař, tel: +420 543 559 254, e-mail: pilar@nconzo.cz.

Dodatečné informace k zadávacím podmínkám včetně přesného znění požadavku jsou zveřejňovány na profilu zadavatele.

Veškeré přílohy zadávací dokumentace jsou zveřejněny a k dispozici ke stažení na profilu zadavatele. Dokumenty ke stažení jsou volně přístupné. Pro další průběh výběrového řízení je vhodná úplná registrace účastníka na portálu Tender arena. Toto je důležité pro následnou evidenci nabídek a veškerou další korespondenci v rámci zakázky.

Adresa profilu zadavatele: <https://www.tenderarena.cz/profil/detail.jsf?identifikator=nconzo>.

12. LHŮTA A MÍSTO PRO PODÁNÍ NABÍDEK

Lhůta pro podání nabídek: Datum: 3. 11. 2022 Hodina: 9:00

Adresa pro podání nabídek: Národní centrum ošetřovatelství a nelékařských zdravotnických oborů, Vlnařská 965/6, PSČ 603 00, Brno

Místo pro příjem nabídek: podatelna v sídle zadavatele, dv. č. 111, budova B,

Nabídku doručte v uzavřené obálce označené:

Veřejná zakázka – „NCO NZO Brno – Systémová ochrana 2022“

na níž bude uvedena kontaktní adresa účastníka, včetně IČ.

na adresu: Národní centrum ošetřovatelství a nelékařských zdravotnických oborů, sekretariát náměstka pro ekonomický a technický úsek, Vlnařská 965/6, PSČ 603 00 Brno.

Nabídku lze na uvedenou adresu doručit osobně. Nabídky zasílané poštou zasílejte tak, aby byly doručeny nejpozději den před lhůtou pro podání nabídek. V den lhůty pro podání nabídek pošta nedoručí zásilky včas (do 9:00 hod). Nabídky doručené po lhůtě nebudou přijaty do výběrového řízení.

13. DALŠÍ ČÁSTI ZADÁVACÍ DOKUMENTACE – PŘÍLOHY

- Příloha č. 1 – Krycí list nabídky.
- Příloha č. 2 – Čestné prohlášení o základní způsobilosti účastníka.
- Příloha č. 3 – Výpočet nabídkové ceny (pouze v elektronické podobě).
- Příloha č. 4 – Souhlas účastníka se zveřejněním budoucího smluvního vztahu.
- Příloha č. 5 – Čestné prohlášení o počtu listů nabídky.
- Příloha č. 6 – Technická specifikace předmětu plnění

Kompletní zadávací dokumentace, včetně všech příloh, je zveřejněna na profilu zadavatele Národní centrum ošetřovatelství a nelékařských zdravotnických oborů na adrese:

<https://www.tenderarena.cz/profil/detail.jsf?identifikator=nconzo>

ID zakázky: VZ0149985

V Brně dne 12. 10. 2022

PhDr.
Michaela
Hofštetrová
Knotková

Digitálně podepsal
PhDr. Michaela
Hofštetrová Knotková
Datum: 2022.10.12
13:49:48 +02'00'

.....
PhDr. Mgr. Michaela Hofštetrová Knotková
ředitelka