OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

# Smlouva
## o poskytnutí licencí a zajištění technické podpory

č.j. objednatele: 2021/OZP/148/0

Smluvní strany:

**Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví**

| | |
|---|---|
| se sídlem: | Roškotova 1225/1, 140 21 Praha 4 |
| zástupce: | Ing. Radovan Kouřil – generální ředitel |
| IČ: | 47114321 |
| DIČ: | XXXXX |

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. A 7232
XXXXX plátcem DPH

dále jen jako „**objednatel**“

a

| ***AEC a.s.*** | |
|---|---|
| se sídlem: | Voctářova 2500/20a, Libeň, 180 00 Praha 8 |
| zástupce: | XXXXX |
| IČ: | 04772148 |
| DIČ: | XXXXX |
| zapsaná v | obchodním rejstříku vedeném u Městského soudu v Praze, spisová zn: B 21326 |
| Bankovní účet | XXXXX |
| je / není plátcem DPH | XXXXX |

dále jen jako „**poskytovatel**“,

### I. Předmět smlouvy

1. Předmětem této smlouvy je povinnost poskytovatele poskytnout licence a čtyřletou technickou podporu k antivirovému software DNS RESOLVER- softwaru pro pro bezpečnost dat a provoz bezpečného e-mail prostředí - specifikovanému v příloze č. 1 této smlouvy (dále jen „software“), a to včetně průběžné a pravidelné aktualizace Softwaru – (dále jen „předmět plnění“).
2. Technická podpora, specifikovaná v článku II. a příloze č. 1 Smlouvy (dále jen „Technická podpora“) bude poskytovatelem poskytována po dobu 4 let od předání software dle čl. II odst. 2 Smlouvy. V rámci Technické podpory zajistí poskytovatel objednateli aktualizace software na nejnovější licencované verze software vydané výrobcem v uvedeném období a podporu pro řešení technických problémů spojených s provozem software v rozsahu a specifikaci dle Přílohy č.1 této smlouvy.
3. Objednatel se zavazuje zaplatit poskytovateli za předmět plnění níže sjednanou odměnu.

### II. Povinnosti poskytovatele

1. Poskytovatel se zavazuje poskytnout objednateli licence k software a předat objednateli licenční ujednání, licenční klíče a potvrzení pro poskytování technické podpory na 4 roky k software ze systému výrobce, to vše nejpozději do 20 dnů ode dne účinnosti této smlouvy.
2. Poskytnutí podkladů dle předchozího odstavce bude potvrzeno podpisem oprávněného zaměstnance objednatele na předávacím protokolu (dále jen „předávací protokol“), přičemž každá ze smluvních stran obdrží 1 jeho výtisk. Návrh předávacího protokolu tvoří **přílohu č. 3** Smlouvy.

3. Při poskytování plnění dle této smlouvy se poskytovatel zavazuje postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností a podle pokynů objednatele. V případě nevhodných pokynů objednatele je poskytovatel povinen objednatele písemně upozornit na nevhodnost jeho pokynů, v opačném případě poskytovatel nese odpovědnost za vady a škodu, které v důsledku nevhodných pokynů vzniknou.
4. Poskytovatel odpovídá za řádné a včasné poskytování služeb dle této smlouvy po celou dobu její účinnosti.
5. Objednatel je oprávněn nahlašovat vady poskytovateli telefonicky nebo emailem na adresu kontaktní osoby poskytovatele uvedené v čl. VII. této smlouvy.
6. Poskytovatel je povinen zahájit práce na odstranění vad nejpozději do druhého pracovního dne od nahlášení závady a odstranit vady do 5 pracovních dnů ode dne jejich nahlášení. V případě, že poskytovatel nezahájí odstraňování vad nebo neodstraní vady ve lhůtách dle předchozí věty, je objednatel oprávněn odstranit vady na vlastní náklady, které je poskytovatel povinen následně objednateli uhradit do 14 dnů ode dne obdržení faktury. Tímto ujednáním není dotčeno právo objednatele na náhradu škody.
7. Poskytovatel se zavazuje informovat objednatele o všech skutečnostech, které by mohly ovlivnit plnění této smlouvy.
8. Poskytovatel je povinen objednateli poskytnout za dobu trvání 4 let technické podpory služby, spočívající v konzultační činnosti a realizaci změnových požadavků, definované v příloze č. 1 smlouvy, a to v celkovém rozsahu 120 hodin. Smluvní strany si po skončení každého kalendářního měsíce prostřednictvím e-mailové k0omunikace kontaktních osob odsouhlasí počet vyčerpaných hodin.

## III. Cena a platební podmínky

1. Podrobná kalkulace ceny je uvedena v příloze č. 2 této smlouvy – Cenová tabulka.
2. Výše ceny je konečná a nepřekročitelná. Součástí ceny jsou veškeré náklady poskytovatele spojené s plněním jeho povinností dle této smlouvy.
3. Cena bude objednatelem zaplacena jednorázově na základě daňového dokladu (v případě, že poskytovatel je plátcem DPH) nebo faktury (v případě, že není platcem DPH) (dále jen „Faktura“). Poskytovatel je oprávněn vystavit Fakturu po podpisu předávacího protokolu dle čl. II. odst. 2 této smlouvy. Splatnost Faktury bude 30 dnů ode dne doručení Faktury objednateli. Má se za to, že lhůta splatnosti byla dodržena, pokud bude odměna poukázaná poskytovateli v den splatnosti odepsána z účtu objednatele.
4. Daňový doklad musí mít veškeré náležitosti v souladu se zákonem o dani z přidané hodnoty, faktura musí mít veškeré náležitosti v souladu se zákonem o účetnictví. Ve Faktuře bude uveden odkaz na tuto smlouvu a její přílohou bude zástupcem objednatele podepsaný předávací protokol. V opačném případě je objednatel oprávněn zaslat Fakturu zpět poskytovateli k doplnění. Lhůta splatnosti odměny začne v takovém případě běžet až od doručení bezvadné Faktury objednateli.
5. V případě, že by hrozilo, že objednatel může ručit za poskytovatelem nezaplacenou daň z přidané hodnoty dle ust. § 109 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, je objednatel oprávněn uhradit část daňového dokladu poskytovatele ve výši vyúčtované daně z přidané hodnoty na bankovní účet místně příslušného správce daně poskytovatele. Takový postup objednatele se v rozsahu částky poukázané na účet správce daně považuje za řádné a včasné uhrazení odměny poskytovateli.
6. Poskytovatel je oprávněn postoupit pohledávku za objednatelem jen s předchozím výslovným písemným souhlasem objednatele.

## IV. Práva duševního vlastnictví

1. Poskytovatel se zavazuje, že při poskytování služeb neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, zejména z autorských práv a práv

průmyslového vlastnictví. Poskytovatel se zavazuje, že objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které objednateli vzniknou v důsledku uplatnění práv třetích osob vůči objednateli v souvislosti porušením povinnosti poskytovatele dle předchozí věty.

2. Poskytovatel výslovně prohlašuje, že je plně oprávněn disponovat právy k duševnímu vlastnictví dle této smlouvy (např. poskytovat podlicence), a zavazuje se za tímto účelem zajistit řádné a nerušené užívání předmětu smlouvy objednatelem, včetně případného zajištění dalších souhlasů a licencí od autorů děl v souladu s autorským zákonem popř. od nositelů jiných práv duševního vlastnictví v souladu s právními předpisy. Veškeré náklady tímto vzniklé jsou součástí ceny za poskytnutí služeb dle této smlouvy.
3. Poskytovatel tímto podle ustanovení § 2358 a násl. občanského zákoníku poskytuje objednateli k užívání veškerého software dle této smlouvy licence, a to jako licence:
   a) nevýhradní, opravňující objednatele k veškerým známým způsobům užívání software, dostačující k běžnému i objednatelem zamýšlenému užívání software a zachování jeho funkčnosti,
   b) platné na dobu neurčitou, neomezené územním či množstevním rozsahem,
   c) převoditelné a postupitelné, tj. s právem udělení podlicence či postoupení licence třetí osobě,
   d) které není objednatel povinen využít.
4. Objednatel nabývá práva z poskytnutých licencí jejich předáním/poskytnutím.

## V. Povinnost mlčenlivosti

1. Poskytovatel je povinen zachovávat mlčenlivost ohledně veškerých důvěrných informací objednatele, které se v souvislosti s plněním této smlouvy dozví. Poskytovatel je povinen zajistit zachování mlčenlivosti i u svých zaměstnanců, zástupců, případně i jiných spolupracujících třetích stran, pokud bylo nevyhnutelné a nezbytně nutné jim takové informace pro účely této smlouvy poskytnout. Poskytovatel se rovněž zavazuje neposkytovat třetím osobám informace o poskytování software (informace o koncovém zákazníkovi).
2. Za důvěrné informace se považují jakékoliv informace, které
   (a) tvoří obchodní tajemství objednatele (skutečnosti obchodní a technické povahy související s činností objednatele), nebo se týkají činnosti objednatele, jeho strategie, know-how, způsobu řízení, vnitřních předpisů a pracovních postupů, nebo
   (b) jsou chráněny nebo podléhají zvláštnímu režimu nakládání na základě příslušných právních předpisů (např. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracovnáním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) nebo závazkových vztahů, jejichž účastníkem je objednatel), nebo
   (c) jsou součástí informačního systému objednatele, nebo se na ně vztahuje povinnost mlčenlivosti ve smyslu ustanovení § 22 zákona č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách, nebo
   (d) budou objednatelem označeny za důvěrné, nebo
   (e) by v případě jejich prozrazení poškodily, nebo mohly objednatele poškodit,

   a které nejsou veřejně dostupné.
3. Poskytovatel se zavazuje:
   a) uchovávat důvěrné informace v tajnosti a nakládat s nimi výlučně v souvislosti s plněním svých povinností dle této smlouvy, při čemž je povinen řídit se pravidly pro nakládání s těmito informacemi, které vyplývají z právních předpisů, interních předpisů nebo rozhodnutí orgánů objednatele,
   b) nevyužít, ani se nepokusit využít důvěrné informace pro vlastní potřebu nebo pro potřebu jakékoliv třetí osoby způsobem, který by byl v rozporu s právními předpisy či s touto smlouvou

nebo jejím účelem nebo by přímo nebo nepřímo jakkoliv poškodil nebo mohl poškodit objednatele.

4. Povinnost mlčenlivosti o důvěrných informacích podle tohoto článku trvá dále i po ukončení této smlouvy.

## VI. Smluvní sankce a možnost odstoupení od smlouvy

1. Pro případ prodlení poskytovatele s poskytnutím licencí k software nebo s předáním podkladů dle čl. II. odst. 1 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 1.500,- Kč za každý započatý den prodlení.
2. V případě prodlení poskytovatele s odstraněním vad podle čl. II. odst. 6 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 1.500,- Kč za každý započatý den prodlení.
3. Pro případ prodlení objednatele s úhradou odměny je objednatel povinen zaplatit poskytovateli úrok z prodlení ve výši 0,05 % z dlužné částky za každý den prodlení.
4. V případě porušení povinnosti mlčenlivosti poskytovatele dle čl. V. této smlouvy se poskytovatel zavazuje zaplatit objednateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení.
5. V případě, že v důsledku byť nezaviněného jednání poskytovatele bude objednateli uložena jakákoli veřejnoprávní sankce či povinnost plnění ve prospěch třetí osoby, je poskytovatel povinen zaplatit objednateli plnou hodnotu této sankce, resp. plnění, zvýšenou o smluvní pokutu ve výši 1 % tohoto plnění.
6. Právo objednatele požadovat ve všech uvedených případech kromě smluvní sankce i náhradu škody není těmito ujednáními dotčeno. Smluvní pokuty dle tohoto článku jsou splatné do 14 dní ode dne doručení písemné výzvy k jejich úhradě povinné smluvní straně.
7. Objednatel je oprávněn od této smlouvy s okamžitou účinností odstoupit v případě, kdy poskytovatel bude v prodlení se splněním některé své povinnosti vyplývající z této smlouvy o více než 15 dní.
8. Odstoupením od smlouvy není dotčen nárok objednatele na náhradu škody v plné výši.

## VII. Závěrečná ujednání

1. Kontaktní osobou objednatele je: XXXXX, tel. XXXXX, e-mail: XXXXX.
2. Kontaktní osobou poskytovatele je: XXXXX, tel. + XXXXX, e-mail XXXXX.
3. Práva a povinnosti plynoucí z této smlouvy se řídí výhradně českým právem. Veškeré případné spory mezi stranami vyplývající nebo související s ustanoveními této smlouvy budou řešeny nejprve smírně. Nebude-li takto dosaženo řešení, je k rozhodování sporů z této smlouvy příslušný obecný soud objednatele.
4. Bude-li některé ustanovení této smlouvy shledáno neplatným či neúčinným, nedotýká se to ostatních ustanovení této smlouvy, která jsou na něm nezávislá a umožňují rozumné plnění smlouvy v souladu s jejím účelem. Smluvní strany se v tomto případě zavazují nahradit ustanovení neplatné či neúčinné novým ustanovením platným a účinným, které odpovídá zamýšlenému účelu neplatného ustanovení.
5. Tato smlouva je vyhotovena ve dvou stejnopisech, po jednom pro každou smluvní stranu. Tuto smlouvu lze měnit či doplňovat pouze vzestupně číslovanými písemnými dodatky, podepsanými oběma smluvními stranami. Všechny v této smlouvě uvedené přílohy jsou její nedílnou součástí.
6. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
7. Smluvní strany po jejím přečtení prohlašují, že souhlasí s jejím obsahem, že smlouva byla sepsána určitě, srozumitelně, na základě jejich pravé a svobodné vůle a bez nátlaku na některou ze smluvních stran. Na důkaz toho připojují smluvní strany své podpisy.

Seznam příloh:

Příloha č. 1 – Specifikace předmětu plnění
Příloha č. 2 – Cenová tabulka
Příloha č. 3 – Vzor předávacího protokolu

V Praze dne: .....

.....
**Ing. Radovan Kouřil**
**generální ředitel**

**Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví**

V Praze dne: ……..

.....
XXXXX
XXXXX
**AEC a.s.**

**Příloha č. 1**
**Specifikace předmětu plnění a kalkulace ceny**

**DNS resolver poskytující překlad externích domén s bezpečnostními moduly.**

---

Všeobecné požadavky na řešení:

- Nevyžaduje modifikaci na koncové stanici:
  - Bez potřeby instalace SW na koncové stanici
  - Bez potřeby manuální rekonfigurace, všechno musí být vykonáváno automaticky
  - Bez potřeby instalace certifikátů nebo přenastavení bezpečnostních politik

Řešení poskytující ochranu na úrovni DNS proti:

- Malware
- Zero – Day detection of Domain generation algorithm
- Phishing
- Homograph phishing attack´s
- C&C
- Exploits
- Spam domains
- Malicious coinmining
- DNS Tunneling
- Cache poisoning
- DNS rebinding attacks
- DNS anomaly detection & alerting

Parametry pro security filtering engine:

- Má nulovou latenci pro uživatele. Security vyhodnocování probíhá v reálném čase bez over-the-network dotazů
- Nasazení software bez potřeby speciálně upraveného hardware. Schopnost fungovat ve virtuálním prostředí
- Ochrana vůči DNS spoofing útokům založeným na DNSSEC včetně NSEC3 podpory a negativního cachingu
- Možnost definovat rozdílné security politiky přirazené sítím založeným na CIDR
- Detekce Zero-day hrozeb bez nutnosti předcházející znalosti dané domény
- Detekce a alerting anomálií v rámci DNS trafficu
- Možnost alertovat / blokovat z vnitřní sítě přístup k doménám vypadajícím podobně jako definovaná doména společnosti pro ochranu při cílených phishingových útocích
- Možnost blokovat přístup k doménám podle kategorie obsahu, alespoň v rozsahu:
  - Coinminers
  - Pornografie
  - Hazard
  - Násilí
  - Tracking
  - Reklama
  - Sociální sítě
  - Hry

- DNS tunneling vrstva poskytuje ochranu proti zneužití DNS provozu pro tunelování jiné komunikace v technicky validních DNS paketech a komunikace s externími servery
- DNS tunneling vrstva proaktivně rozbíjí DNS tunneling na více úrovních:
  - resolver
  - neuronová síť

- Politiky umožňují administrátorům upravit:
  - Úroveň ochrany

- Úroveň detekce
- Kategorie hrozeb jsou zahrnuty v konkrétních politikách
- Vlastní blacklisty a whitelisty
- Blokované kategorie obsahu

**Funkce a komponenty**

On-premise resolver:

- Plně autonomní DNS resolver se security vrstvou, tedy schopný dělat samotný resolving a filtering, bez potřeby komunikace s externí službou v cloudu
- Security vrstva umožňuje přesměrování požadavku na závadné domény na blokační stránku
- Blokační stránka
  - Je webová stránka, kam je uživatel přesměrován, když se on nebo jeho zařízení snaží přistoupit na závadnou webovou stránku
  - Blokační stránku je možné jakkoli upravit dle přání objednatele
  - Funkce “Bypass” pro definované sítě – uživatele umožňuje pokračovat na cílovou doménu bez nutnosti spolupráce administrátora (např. pro guest sítě)
- Splňující RFC standardy
- Podporující DNSSEC validation včetně NSEC3 negative caching
- Konfigurační změny a update resolverů se vykonávají za plného provozu – bez DNS traffic výpadku při updatu a rekonfiguraci
- DNS traffic management a firewalling
  - Konkrétní zóny mohou být přesměrovány na vybrané IP adresy
  - DNS cache prefetching – záznamy v mezipaměti jsou obnoveny předtím než expirují
  - DNS záznamy jsou drženy v paměti déle, než by kvůli ttl periodě měli být autoritativní nameservers pro zónu nedostupné (e.g. domain.com je nedostupná během jedné hodiny, resolver bude schopný použít poslední odpověď, kterou měl pro tuhle doménu).
  - DNS Firewall – možnost definovat pravidla přístupu na konkrétní domény – povolení přístupu jen na vybrané domény per IP subnet. Příklad využití – povolení přístupu pro klientské stroje jen na domény Office 365, na ostatní vrátit odpověď NXDOMAIN.
  - Automatická aktualizace záznamu domén Office 365 a dalších služeb Microsoft Azure použitých v DNS firewallu
- Podporující využití DNS over TLS a DNS over HTTPS

Centrální management:

- Zobrazuje kompletní DNS traffic v reálném čase
- Poskytuje a vykonává:
  - Update databáze per security filtering,
  - Management resolverů a softwarových updatů
  - Centrální úložiště logů a incidentů a poskytuje možnosti pro jejich vyhodnocování
- DNS Traffic log včetně detailů o všech unikátních požadavcích / odpovědích pro další analýzu jsou přístupné a exportované ze všech resolverů ve společnosti a dostupné včetně fulltextového filtrovaní v jednom rozhraní (např. v csv formátu)
- Možnost analyzovat doménu z pohledu bezpečnosti a obsahu včetně integrace na bezpečnostní služby třetích stran
- Alerting upozorňující na anomálie detekované v rámci DNS Trafficu
- Alerting a reporting doručovaný pomocí:
  - E-mail
  - Syslog (TLS)

    - Slack
    - RESP API
- DNS traffic overview umožňuje komplexní analýzu DNS komunikace včetně detailního:
    - drilldownu jednotlivých událostí
    - filtrování
    - exportu dat
    - přehledu trendů
- Lokalizován v jazycích:
    - Čeština
    - Slovenština (volitelně)
    - Angličtina
    - další na vyžádání

Administrátorské rozhraní:

- Webové rozhraní pro administrátora je plně přístupné přes moderní webové prohlížeče bez potřeby doinstalování add-ons nebo lokálního software potřebného pro přístup do rozhraní
- Možnost aktivace dvoufaktorové autentizace a vynucení dvoufaktorové autentizace pro všechny administrátory v organizaci
- Dostupnost nápovědy a dokumentace
- Rozdílné nastavení oprávnění (pro jednotlivé skupiny) dostupné pro operátory přinejmenším ve 2 rolích:
    - Administrátor
    - Uživatel s oprávněním pro čtení
- DNS traffic log ze všech resolverů je dostupný včetně fulltextové filtrace v jednotném rozhraní
    - Detaily o všech unikátních požadavcích/odpovědích budou přístupné a exportovány pro další analýzu v .csv formátu
- Administrátorské webové rozhraní poskytuje přístup do všech funkcí:
    - Threat analysis
    - DNS traffic analysis
    - Security filtering configuration
    - DNS resolver management
    - Alerting
    - Možnost tvorby vlastních whitelistů a blacklistů
- Lokalizováno v jazycích:
    - Čeština
    - Angličtina
    - Slovenština (volitelné)

DNS resolver management poskytuje:

- Vzdálenou diagnostiku:
    - Monitorování hardwarových problémů
    - Softwarový monitoring
    - Sběr logů
    - Vyhodnocování latence překladu
- Softwarové updates a rollbacks:
    - Možnost okamžitě vykonat rollback libovolného update do předcházejícího stavu
- Lokální management
    - Plný přístup k logům pro lokální administrátory
    - Lokální CLI

Alerting:

- Konfigurovatelné filtry pro domény, sítě, akce
- Početné možnosti doručení a protokoly pro doručení alertů, které zahrnují:
    - E-mail
    - Syslog (TLS)
    - Slack
    - Webhook (REST API)
    - Dodatečná cílové místa doručení alertů (na vyžádání)
- Alertování je založeno na
    - Thresholdech security událostí a DNS trafficu
    - Detekci dynamických anomálií
    - Whitelistech a blacklistech

Reporting:

- Reporty jsou dodávány pomocí e-mailu
- Průběžné reporty sumarizují
    - Objemy provozu
    - Množství hrozeb dle jednotlivých kategorií
    - Podezřelá a nakažená klientská zařízení
    - Převládající rodiny škodlivého kódu a závadných domén

Integrační procesy:

- Dostupnost REST API pro získaní informací
    - Detaily o událostech a hrozbách
    - Statistiky DNS provozu
    - REST API parametry pro filtrování založené na:
        - Zdrojové IP adrese
        - Destination domain
        - Typu požadavku
        - Typu hrozby
        - IP adrese odpovědi
        - Čase

- Syslog integrace (SIEM, log management, provozní monitoring apod.)
    - Konfigurovatelný tok dat přes syslog obsahující detekované hrozby
    - Konfigurovatelný tok dát přes syslog obsahující DNS provoz

Dodání řešení:

- objednanou technologii je možno dodat do 48 hodin od zaslání závazné objednávky, příp. podepsání smlouvy

Implementace řešení:

- technologie je instalována a zapojena do stávající síťové infrastruktury bez plánovaného výpadku nebo odstávky
- integrace s technologiemi jako: MS AD, SIEM, Log manager, Provozní monitoring, Flowmon ADS,

Rozsah poskytované technické podpory:

- Vzdálená podpora výrobce (mail, telefonicky, ticketovacím nástrojem) v lokálním jazyce: česky/anglicky, anglicky (dle preferencí objednavatele)
- Poskytnutí podpory na místě do 4 hodin od nahlášení v případě kritických problémů

Dokumentace:

- Technická dokumentace k řešení je lokalizována do jazyků:
  - Čeština
  - Angličtina
  - Slovenština (volitelně)
  - Dle požadavků

**Všeobecný popis implementačních prací**

Popis prací během nasazení řešení:

- Příprava infrastruktury a součinnost:
  - Dodavatel uvede systémové požadavky a rozsah součinnosti pro implementaci řešení

- Dodavatel zodpovídá za:
  - Implementaci řešení v prostředí objednatele
  - Integraci s vybranými technologiemi objednatele
  - Zaškolení administrátorů objednatele

- Kontrola kvality
  - Kontrola kvality nastavení systému ze strany výrobce řešení po implementaci řešení smluvním dodavatelem je součástí dodaných prací

- Záruka
  - údržba SW, zákaznická podpora telefonicky a e-mailem v českém/slovenském a anglickém jazyce min. v pracovní době (9x5), přístup k webovému zákaznickému centru, vzdálená podpora přes SSH

- Další podmínky realizace
  - Konfigurace alertů pro vážné bezpečnostní incidenty jako:
    - Cílený phishingový útok - homograph & typosquatting attack
    - Komunikace infikovaného stroje s řídícím serverem botnetu - C&C server
    - Aktivita Zero day malware – přinejmenším ve formě Domain generation algorithm malware

  - Konfigurace alertů pro provozní incidenty:
    - Selhání DNS překladu
    - Saturace systémových zdrojů na infrastruktuře, na které je nainstalována technologie

  - Implementovaná technologie je plně podporovaná výrobcem. Je potřebné garantovat vyvarování se porušení podmínek, které by mohly porušit podmínky podpory stanovené výrobcem.

- Bezvýpadková instalace technologie a její zapojení do stávající síťové infrastruktury.

- Integrace:
  - Integrace s Active Directory a zajištěním funkcionality všech interních systémů, doménových řadičů a klientských aplikací
  - Zasílání událostí do SIEM řešení nebo do technologie pro management logů
  - Zasílání informací o provozních problémech e-mailem nebo do helpdesku
  - Možnost čtení a filtrace událostí přes API (preferováno je REST API)
  - Řešení musí být možné v budoucnu integrovat – musí podporovat integraci s technologií pro detekci anomálií v síťovém provozu

## Konzultační činnost

- Poradenská činnost při detekci a vyhodnocování incidentů
- tvorba pravidelných sumárních reportů za delší časové období (např. kvartálně
- online/onsite prezentací včetně:
  - zhodnocení trendů v rámci DNS traffic
  - analýza provozních a bezpečnostních anomálií identifikovaných v rámci DNS traffic
  - analýza vážných bezpečnostních incidentů, které DNS Resolver zaznamenalo a zablokoval
  - návrh doporučení pro další konfiguraci řešení
  - individuální analýza vážných bezpečnostních incidentů, které DNS Resolver zaznamenalo a zablokoval

## Realizace změnových požadavků

**Změny konfigurace:**

- úprava bezpečnostních politik
- tvorba nových bezpečnostních politik pro vybrané subsegmenty datové sítě resp. vybrané síťové rozsahy
- tvorba nových bezpečnostních, nebo provozních alertů
- úprava existujících provozních alertů
- tvorba šablony reportingu
- custom upravené reportingové šablony

**Integrace dalších bezpečnostních a provozních technologií:**

- Flowmon ADS
- Novicom
- Open DXL vrstva
- tvorba nových korelačních anebo parsovacích pravidel pro SIEM technologie (Log manager)

**Úprava nastavení již integrovaných bezpečnostních technologií**

**Integrace nestandardních technologií (zatím nedefinovaných)**

*Příloha č. 2 Smlouvy – Cenová tabulka*

## Cenová tabulka

| Položka cenové kalkulace | Počet licencí | Cena v Kč bez DPH | DPH 21% | Cena v Kč vč. 21 % DPH |
|---|---|---|---|---|
| Licence Software DNS RESOLVER | 600 | 460 800 | 96 768 | 557 568 |
| Technická podpora licencí software DNS RESOLVER 4 ROKY | 600 | 691 200 | 145 152 | 836 352 |
| Implementace řešení a napojení na systémy OZP, včetně LOGmanageru | - | 80 500 | 16 905 | 97 405 |
| Cena za realizaci změnových požadavků a konzultačních hodin v rozsahu 120 hodin za 4 roky | - | 396 000 | 83 160 | 479 160 |
| **Cena celkem bez DPH:** | 1 628 500 | | | |
| **Cena celkem včetně DPH:** | 1 970 485 | | | |

*Příloha č. 3 Smlouvy – Vzor předávacího protokolu*

# PROTOKOL č.

## a) o převzetí Plnění

**Předmět plnění:**

| Označení | Název/Popis | Množství | Identifikace |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | |
|---|---|
| **Č. objednávky/smlouvy OZP:** | |
| **Datum převzetí:** | |

| | |
|---|---|
| **Poskytovatel:**<br><br>**Podpis:** | **Objednatel:**<br><br>**Podpis:** |