Kupní smlouva č. 1138/2023
na dodávku softwarových produktů

uzavřená podle příslušných ustanovení zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) a s přihlédnutím k příslušným ustanovením zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

Smluvní stany:

Město Znojmo
se sídlem: Obroková 1/12, 669 02 Znojmo
zastoupené: Ing. Ivana Solařová, starostka
kontaktní osoba: Ing. Lubomír Otepka, vedoucí oddělení informatiky
IČO: 00293881
DIČ: CZ00293881

(dále jen „**Kupující**“)

a

PCS spol. s r.o.
se sídlem: Na Dvorcích 122/18, 140 00 Praha 4
zastoupená: Ing. Petr Vašák, jednatel společnosti
kontaktní osoba: Bohdan Vrabec, ředitel divize DataGuard
IČO: 00571024
DIČ: CZ00571024
zapsaná v obchodním rejstříku u Městského soudu v Praze, sp. zn. oddíl C, vložka 527

(dále jen „**Prodávající**“)

uzavírají níže uvedeného dne, měsíce a roku tuto kupní smlouvu (dále jen „smlouva“):

Čl. I
Účel a předmět smlouvy

1. Předmětem této smlouvy je závazek Prodávajícího za podmínek stanovených touto smlouvou dodat Kupujícímu nevýhradní licence k užití softwarových produktů pro **antimalware zabezpečení**, a to dle specifikace uvedené v příloze č. 1 této smlouvy (dále též **„softwarové produkty“**). Kupující se naproti tomu zavazuje softwarové produkty převzít a zaplatit za poskytnuté plnění Prodávajícímu kupní cenu stanovenou podle Čl. IV této smlouvy.

2. Prodávající se dále zavazuje k poskytnutým softwarovým produktům poskytovat služby lokální technické podpory, a to v rozsahu specifikace uvedené v příloze č. 1 této smlouvy.

Cena za poskytování služeb lokální technické podpory je součástí kupní ceny za poskytnuté plnění dle Čl. IV této smlouvy.

3. Součástí předmětu plnění je vedle dodávky nevýhradní licence k užití softwarových produktů pro antimalware zabezpečení kompletní instalace, uvedení software do provozu a instruktáž obsluhy s předvedením funkčnosti a lokální technická podpora, tj. v souladu s požadavky sjednanými v příloze č. 1.

Čl. II
Práva a povinnosti smluvních stran

1. Prodávající se zavazuje dodat Kupujícímu softwarové produkty a služby technické podpory za podmínek stanovených touto smlouvou.
2. Kupující se zavazuje poskytnuté plnění převzít a zaplatit Prodávajícímu odměnu stanovenou podle čl. IV odst. 1 této smlouvy.
3. Smluvní stany se zavazují informovat se navzájem o všech skutečnostech, které by, mají nebo by mohly mít vliv na plnění této smlouvy.
4. Smluvní stany jsou povinny poskytovat si nezbytnou součinnost k bezvadnému plnění této smlouvy.

Čl. III
Mechanismus dodávek

1. Prodávající se zavazuje dodat softwarové produkty a služby ve prospěch Kupujícího nejpozději do 10 dnů od účinnosti této smlouvy. Softwarové produkty je Prodávající povinen dodat Kupujícímu elektronicky na kontaktní adresu: lubomir.otepka@muznojmo.cz nejpozději do 10 dnů ode dne podpisu této smlouvy smluvními stranami. Implementace dle přílohy č. 1 Technická specifikace softwarového produktu bodu G. nejpozději do 60 dnů ode dne účinnosti této smlouvy.
2. Místem plnění je sídlo Kupujícího na adrese: **Obroková 1/12, 669 02 Znojmo**. Doprava je zahrnuta v odměně dle Čl. IV této smlouvy.
3. Kupující je povinen řádně a včas dodané softwarové produkty od Prodávajícího, za podmínek stanovených touto smlouvou, převzít a zaplatit cenu dle Čl. IV odst. 1. této smlouvy.
4. Prodávající se zavazuje poskytovat technickou podporu k předmětu smlouvy po dobu 36 měsíců ode dne dodání předmětu smlouvy Kupujícímu. Náklady na technickou podporu jsou zahrnuty v kupní ceně.

Čl. IV
Cena a odměna za poskytnutí podlicence

1. Celková kupní cena za poskytnutí softwarových produktů a služeb dle Přílohy č. 2 této smlouvy je stanovena na základě nabídkové ceny Prodávajícího ze dne 24.11.2023, kalkulované v rámci zadávacího řízení na veřejnou zakázku, která předcházela uzavření této smlouvy, jako cena nejvýše přípustná a činí částku ve výši **647.408 Kč bez DPH (slovy: šest set čtyřicet sedm tisíc čtyři sta osm korun českých), DPH 135.955,68 Kč, cena včetně DPH: 783.363,68 Kč**. Pokud by došlo ke změně sazby DPH, bude tato sazba a výše ceny s DPH

příslušně upravena.

2. Cena Prodávajícího zahrnuje veškeré náklady související s plněním Prodávajícího, tj. zejména dopravu, mzdy zaměstnanců, pojištění apod.

Čl. V
Platební podmínky

1. Kupující nebude Prodávajícímu poskytovat zálohy.
2. Kupující uhradí cenu za předmět plnění dle této smlouvy na základě řádného daňového dokladu vystaveného Prodávajícím. Prodávající vystaví fakturu za dodávku software (rozsah definován v příloze č. 1 Technická specifikace softwarového produktu bodech A až F této smlouvy) nejpozději do 25. 12. 2023. Faktura za implementaci (rozsah definován v příloze č. 1 Technická specifikace softwarového produktu bodu G této smlouvy) bude vystavena po dokončení implementace.
3. Daňový doklad (faktura) bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a bude mít náležitosti obchodní listiny ve smyslu ust. § 435 občanského zákoníku. Faktura musí obsahovat číslo této smlouvy a číslo objednávky Kupujícího. Součástí faktury je i oboustranně podepsaný předávací protokol. Pokud faktura nebude splňovat všechny uvedené náležitosti a přílohy, má Kupující právo fakturu vrátit k doplnění. V takovém případě nastane splatnost kupní ceny až dnem, který je jako den splatnosti vyznačen v dodatečně doručené řádné faktuře.
4. Splatnost daňového dokladu činí 30 dnů ode dne jeho vystavení, min. 14 dní ode dne doručení objednateli.
5. Prodávající je povinen doručit fakturu na adresu:

   Město Znojmo
   Ing. Lubomír Otepka
   Obroková 1/12
   669 02 Znojmo

   nebo v elektronické podobě na adresu kontaktní osoby uvedené v Čl. VI této smlouvy.
6. Povinnost Kupujícího zaplatit je splněna dnem odepsání příslušné částky z účtu Kupujícího na účet Prodávajícího.

Čl. VI
Kontaktní osoby

1. Kontaktní osobou Kupujícího je:
   Ing. Lubomír Otepka, e-mail: lubomir.otepka@muznojmo.cz, telefon: +420 603 888 385
2. Kontaktní osobou Prodávajícího pro záležitosti obchodní je:
   Bohdan Vrabec, e-mail: b.vrabec@pcs.cz, telefon: + 420 603 985 726

Čl. VII
Záruka za jakost

1. Prodávající se zavazuje, že softwarové produkty a služby budou po dobu, na kterou bude poskytnuta licence, způsobilé pro použití ke smluvenému účelu a že si zachovají smluvené a jinak obvyklé vlastnosti. Záruka za jakost softwarových produktů a služeb činí 36 měsíců a její běh počíná od data platnosti licence softwarového produktu.

2. Prodávající je povinen v průběhu záruční doby bezplatně a neprodleně odstraňovat závady související s poskytováním softwarových produktů a služeb po jejich nahlášení servisnímu středisku Prodávajícího.
3. Servisní středisko Prodávajícího pro hlášení závad Help desk: https://dataguard.atlassian.net/servicedesk, kontaktní telefon +420 296 796 100, e-mail: dataguard@pcs.cz.
4. Prodávající se zavazuje v průběhu záruční doby odstranit závadu na softwarových produktech a službách dle lhůt stanovených v příloze č. 2 této smlouvy, přičemž uvedená lhůta počíná běžet od data písemného nahlášení závady Prodávajícímu. Prodávající neodpovídá za závady, které vyžadují programátorský zásah do softwarového produktu, který může provést pouze jeho výrobce.

Čl. VIII
Prodlení, sankce

1. V případě ocitne-li se Prodávající v prodlení s jakoukoli dodávkou softwarových produktů a služeb podle čl. III této smlouvy, je Kupující oprávněn požadovat po Prodávajícím uhrazení smluvní pokuty ve výši 0,5 % za porušení každé povinnosti uvedené v čl. III této smlouvy, a to za každý i započatý den prodlení.
2. Jestliže je Kupující v prodlení s plněním povinnosti dle Čl. V odst. 4. této smlouvy, je Prodávající oprávněn požadovat po Kupujícím smluvní úrok z prodlení ve výši 0,5 % za každý i započatý den prodlení.
3. Kupující se zavazuje Prodávajícímu poskytovat po celou dobu platnosti této smlouvy potřebnou součinnost pro plnění jeho závazků vyplývajících z této smlouvy. Neposkytování potřebné součinnosti ze strany Kupujícího omezuje právo Kupujícího nárokovat na Prodávajícím odpovídající sankce za prodlení dle této smlouvy.

Čl. IX
Platnost, změna, a zánik smlouvy

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem zveřejněním v registru smluv.
2. Obsah smlouvy může být měněn jen dohodou stran smluvních, a to vždy jen vzestupně číslovanými písemnými dodatky potvrzenými oprávněnými zástupci smluvních stran.

Čl. X
Závěrečná ustanovení

1. Práva a povinnosti touto smlouvou výslovně neupravené se řídí občanským zákoníkem.
2. Kupující potvrzuje, že u právních úkonů obsažených v této smlouvě byly ze strany Kupujícího splněny veškeré tímto zákonem či jinými obecně závaznými právními předpisy stanovené podmínky ve formě předchozího zveřejnění, schválení či odsouhlasení, které jsou obligatorní pro platnost tohoto právního úkonu.
3. Smluvní strany podpisem této smlouvy berou na vědomí, že Kupující je povinným subjektem v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a v souladu se zákonem 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 a že je povinen tuto smlouvu včetně jejích možných

změn a dodatků zveřejnit za zákonem stanovených podmínek, případně informace v ní obsažené nebo z ní vyplývající. Smlouvu se v registru smluv zavazuje zveřejnit Kupující.

4. Obě strany potvrzují, že případné osobní údaje fyzických osob uvedené v této smlouvě nebo vzájemně sdělené v rámci plnění smlouvy byly poskytnuty dobrovolně. Obě strany prohlašují, že veškeré osobní údaje fyzických osob získané v souvislosti s plněním této smlouvy zpracují pouze k účelu danému touto smlouvou, bez využití jiného zpracovatele údajů.
5. Smlouva se vyhotovuje elektronicky.
6. Uzavření této smlouvy schválila Rada města Znojma na své schůzi konané dne 4. 12. 2023, usnesením č. 55/2023, bodem č. 1883.
7. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, s jejím obsahem souhlasí, že smlouva je v souladu s jejich svobodnou vůlí a smlouvu nepodepisují v tísni a za nápadně nevýhodných podmínek. Na důkaz toho připojují své elektronické uznávané podpisy.

Seznam příloh

Příloha č. 1 - Technická specifikace softwarového produktu.
Příloha č. 2 - Položkový rozpočet.

Za Kupujícího:

Elektronický podpis : 8.12.2023
Certifikát autora podpisu :
Jméno : Ing. Ivana Solařová
Vydal : PostSignum Qualified CA 4
Platnost do : 23.11.2025 08:35:07 +01'00

.....
Město Znojmo
Ing. Ivana Solařová
starostka

Za Prodávajícího:

Ing. Petr Vašák
Digitálně podepsal Ing. Petr Vašák
Datum: 2023.12.07 10:25:51 +01'00'

.....
PCS spol. s r.o.
Ing. Petr Vašák
jednatel společnosti

Příloha č. 1 - Technická specifikace softwarového produktu

Specifikace jednotlivých položek dodávky
Nabízené řešení od společnosti Kaspersky splňuje veškeré technické požadavky a požadavky na poskytovanou podporu uvedené v zadávací dokumentaci k veřejné zakázce s názvem „Dodávka antimalware zabezpečení“

Stávající licence:
Kaspersky Endpoint Security ADVANCED (310 lic.)
Kaspersky Endpoint Security SELECT (40 lic.)
Kaspersky Security for Mail Server (450 lic.)
Kaspersky Hybrid Cloud Security (30 lic.)

Dodávané licence:
Upgrade na Kaspersky EDR Optimum (310ks na 3roky)
Kaspersky Endpoint Security SELECT (40ks na 3roky)
Kaspersky Hybrid Cloud Security (30ks na 3 roky)
Kaspersky Securty for MS Office 365 (450ks na 3 roky)

Technická specifikace:

A) Obecné požadavky

Požadavek
Nabízené Endpoint Protection řešení splňující dále požadovaná kritéria pro ochranu stanic, serverů, virtuálního prostředí, BYOD mobilních zařízení včetně MS 365 pošty (v případě MS 365 lze nabídnout SaaS od stejného výrobce jako je nabízené řešení) je vzájemně plně integrováno a je od stejného výrobce.
Nabízená technologie byla testována v nezávislých testech AV Comparatives, www.av-comparatives.org, kategorie Enterprise/Real-World Protection Test za rok 2023
Plná lokalizace GUI rozhraní aplikace na koncových zařízeních typu PC, notebook nebo BYOD mobilní zařízení v češtině.
Bezpečnostní cloud infrastruktura výrobce nabízeného řešení využívaná pro detekci malware mimo prostředí klienta je na území EU nebo některého z přidružených států v Evropě.

B) Pokročilá endpoint ochrana pracovních stanic a serverů rozšířená o funkce EDR (XXX Windows/Linux/Mac desktop OS, XX Windows/Linux serverů)

Požadavek
Podpora pro OS Windows 7 a výše, Windows Server 2008 a výše, Linux (CentOS, Debian, RedHat, Ubuntu, SUSE), Mac.
Rozhraní klientské části endpoint protection je plně lokalizováno do ČJ
APT ochrana (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoků.
Ochrana před exploitací instalovaných aplikací a OS
Pokročilá detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning)
Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce)
Kontrola paměti a detekce Fileless Threats ve Windows.
Podpora MS AMSI Protection Provider.
Antiransomware - detekce pokusů o neoprávněné šifrování dat na úrovni Windows serverů.

Roll-back nechtěných změn v systému v reakci na detekované aktivity malware.
Automatická integrovaná cloud Sandbox ochrana od stejného výrobce jako je dodané řešení
Funkce EDR a rozšíření informací o zjištěných detekcích a další související systémové události jako je vizualizace incidentu formou grafického znázornění vývoje a realizace bezpečnostní hrozby (kill chain), informace o zařízení (IP, MAC, Users, OS, …), způsobu detekce, změnách v registru, stažených souborech, provedených reakcích, informace o procesech, síťových spojeních, atd.
Možnost generování IoC informací na základě zjištěných detekcí s možností spuštění IoC scanu na všechny endpointy a rychlé reakce na zjištěné detekce
Možnost doplnění vlastních IoC detekcí
Podpora rychlé reakce z centrální konzole na zjištěné incidenty a detekce např. blokování spuštění aplikace, izolace zařízení, smazání podezřelého souboru, ukončení procesu, odeslání do karantény, spuštění systémového scanu, provedení CMD příkazu, spuštění IoC scanu.
Možnost konfigurovat firewall pravidla ve Windows Server a Linux prostřednictvím centrální konzole nabízeného řešení
Manuální a plánované spouštění skenování, blokování skriptů, kontrola Windows registrů, Buffer overflow ochrana a skenování na pozadí
Self-Defense ochrana heslem před neoprávněnou deaktivací endpoint protection & EDR ochrany včetně blokování neoprávněné vzdálené správy
Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE)
Pravidelná automatická aktualizace systému (v závislosti na síťovém prostředí se aktualizace stahují buď z centrálního uložiště, nebo přímo z Internetu). Lokální aktualizační servery (mirrory) si mohou vzájemně replikovat data. Pro externí pracovníky lze nastavit sekundární profil aktualizace z internetu.
Centrálně konfigurovaný personální firewall + Host Intrusion Prevention (HIPS). Pravidla firewallu lze automaticky měnit v závislosti na prostředí
Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook
Inspekce síťového provozu HTTP(S) a FTP
Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu
Kontrola URL vůči globální cloudové službě výrobce
Uživatelské bezpečnostní politiky zvlášť na zařízení, web a aplikace.
Application Control – možnost povolovat/blokovat spouštění vybraných aplikací dle nastavené firemní politiky (blacklisty/whitelisty)
Whitelist aplikací na základě digitálního certifikátu, HASH, souborového umístění nebo výrobcem předdefinovaných kategorií
Device Control - možnost blokovat vybraná USB a jiná přídavná zařízení na úrovni sběrnice s možností whitelist zařízení a řízení oprávnění (read/write)
Automatická kategorizace připojovaných USB zařízení dle jejich typu, možnost blokace upravených USB zařízení emulujících standardní klávesnici
Automatická kontrola výměnných zařízení a blokace spuštění spustitelných souborů
Možnost skenování stanice na vyžádání, možnost definovat vytížení koncového bodu a vynechat již dříve zkontrolované a nezměněné objekty
Umožňuje uložit protokoly o činnostech v běžných formátech (CSV, text, Windows event log)
Vlastní šifrování celého disku vč. OS (Full Disk Encryption), výměnných paměťových úložišť a/nebo správa nativního šifrování ve Windows MS BitLocker a v MacOS FileVault.
Data Recovery šifrovaných zařízení v případě havárie včetně centrální správy šifrovacích klíčů
Podpora multifaktorové autentizace v preboot režimu u šifrovaných zařízení
Patch Management - přehled zranitelností u min. 100+ aplikací, včetně možnosti automatické instalace příslušných oprav a aktualizací s podporou jejich agregace
Možnost instalace pouze administrátorem schválených aktualizací s možností využít testovací režim na nastavitelném vzorku zařízení
EDR agent je integrální součást endpoint protection klienta
EDR agent podporuje ovládání prostřednictvím CMD rozhraní
Funkčnost systému ochrany bez nutnosti připojení k centrální správě či internetu, přičemž nedochází k významné degradaci detekčních schopností endpoint protection zabezpečení

C) Ochrana a správa mobilních zařízení typu SmartPhone/tablet (XX mobilních zařízení s Android/iOS)

Požadavek
Podpora pro OS Android a iOS
Podpora cloud centrální správy a nasazení
Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení)
Detekce root/jailbreak zařízení
SMS/MMS AntiSpam a filtr nevyžádaných hovorů
Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace)
Zabezpečení on-line komunikace (firewall)
Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií
Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů
Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět
Správa zařízení - povolení/blokování použití paměťových karet, kamery, WiFi, Bluetooth, IR, …
Příprava zařízení, centrální nastavení politik

D) Optimalizovaná ochrana pro virtuální prostředí (XX virtuálních serverů VMware/Hyper-V)

Požadavek
Optimalizované skenování ve virtuálních prostředí VMware, Hyper-V, Citrix
Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy
Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací
Kontrola poštovní (IMAP, SMTP, POP3, NNTP) a síťové komunikace HTTP(S) a FTP(S)
Podpora MS AMSI Protection Provider
Kontrola integrity systémových souborů, logů a kritických aplikací
Přenesení skenovacích úloh a tím i zatížení na samostatnou virtuální appliance a eliminace opakovaného skenování nezměněných objektů
Application Control – možnost omezit oprávnění běžících aplikací na základě jejich reputace
Roll-back nechtěných změn v systému v reakci na detekované aktivity malware.
Vestavěný firewall a Host Intrusion Prevention (HIPS)
Device Control – správa připojování výměnných zařízení
Podpora integrace s EDR řešením od stejného výrobce

E) Zabezpečení pošty MS 365 (XXX mailových schránek, možnost SaaS od stejného výrobce)

Požadavek
Plně cloudové nasazení s MS Exchange Online integrací nebo služba typu SaaS od stejného výrobce jako je nabízené řešení
Antimalware, antiphishing a antispam ochrana elektronické pošty
Podpora poštovních autentizačních metod SPF, DKIM a DMARC
Detekce Office souborů s makry a možnost blokace
Antimalware kontrola schránky na vyžádání

F) Centrální správa

Požadavek
Konzole centrální správy v provedení cloud webové konzole
Společná konzole pro administraci a analýzu informací jak pro endpoint protection, tak i EDR
Podpora Windows Server 2008 R2 a výše, MS SQL Server 2014 (Express) a výše, MySQL 5.7 a výše
Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC a serverech včetně mobilních zařízení typu SmartPhone a tablet
Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku
Instalace endpoint aplikace na serverech bez nutnosti restartu
Zabezpečené spojení mezi serverem centrální správy a endpoint agenty včetně EDR
Podpora manuální/automatické instalace/odinstalace nekompatibilních aplikací (vč. současné ochrany Kaspersky)
Podpora Active Directory a IPv6
Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin.
Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer.
Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie
Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace).
Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě
Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti.
Podpora virtuálního prostředí (VMware, Hyper-V, Citrix)
Možnost prohlížení všech bezpečnostních událostí na spravovaných zařízeních v síti.
Notifikace pomocí e-mail, syslog, SIEM.
Možnost generovat a odesílat reporty e-mailem ve formátu .PDF nebo .CSV včetně možnosti jejich přizpůsobení.

G) Služby lokální technické podpory

Požadavek
Instalace a konfigurace SW v prostředí Zadavatele. Nastavení centrální správy (včetně pravidel a politik pro všechna zařízení, reporting, alerting, revize aktuálních výjimek)
Revize stávajícího nastavení a přenesení do nabízeného řešení
Nastavení optimalizovaného skenování s ohledem na nízké systémové zatížení ve virtuálním prostředí VMware / Hyper-V dle doporučení výrobce a dostupných funkcí dodaného řešení
Úvodní zaškolení obsluhy na správu a používání dodaného systému
Lokální technická podpora dodavatele nabízeného řešení v ČJ v rozsahu HOT LINE (e-mail/telefon) v pracovních dnech od 8:00 hod. – 16:00 hod.

Příloha č. 2 - Položkový rozpočet.

Název položky	*Počet ks/kpl*	*Cena celkem bez DPH*	*Cena celkem vč. DPH*
Upgrade na EDR Optimum	310	*332 091,00*	*401 830,11*
Endpoint Security	40	*27 515,00*	33 293,15
Hybrid Cloud Security	30	*58 964,00*	*71 346,44*
Securty pro MS Office 365	450	*228 838,00*	276 893,98
Součástí ceny je doručení příslušné licence, implementace, 3letá podpora.			
	Úhrnná cena	**647 408,00**	***783 363,68***