SML 2024/476

Smlouva o dílo
na dodávku a implementaci systému pro ochranu koncových stanic a serverů – EDR

Strany

městská část Praha 12
se sídlem: Generála Šišky 2375/6, 143 00 Praha 4 – Modřany,
zastoupená: Ing. Vojtěchem Kosem, MBA, starostou
IČO: 00231151
DIČ: CZ00231151
bankovní spojení: Česká spořitelna, a.s.
číslo účtu: 000027–2000762389/0800

(dále jen „*objednatel*“)

a

ALTEPRO solutions a.s.
se sídlem: Na Maninách 1092/20, 170 00 Praha 7
zastoupená: Vladimírem Fialou, jednajícím na základě plné moci
IČO: 03665496
DIČ: CZ03665496
bankovní spojení: Komerční banka, a.s.
číslo bankovního účtu: 107-9161070297/0100
zapsaná v obchodním rejstříku sp. zn.: B 20333 vedená u Městského soudu v Praze

(dále jen „*zhotovitel*“)

uzavírají tuto **smlouvu o dílo** v souladu s ustanovením § 2586 a souvisejícími zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „*smlouva*“).

I.
Předmět smlouvy

1. Předmětem této smlouvy je

   1.1. závazek zhotovitele řádně a včas

   - **dodat** systém pro zvýšení kybernetické bezpečnosti koncových stanic a serverů – EDR řešení (licence pro 300 koncových stanic a 50 serverů) v souladu s požadovanou technickou specifikací uvedenou v příloze č. 1; součástí dodávky je instalace a implementace do prostředí IS ÚMČ Praha 12 (zhotovitelem dodaný systém dále jen jako „**EDR řešení**“ nebo „**dílo**“),
   - bezodkladně po instalaci a implementaci začít **poskytovat technickou podporu** (dle specifikace v čl. XI. této smlouvy a v příloze č. 1 této smlouvy, dále jen „**technická podpora**“);

   1.2. závazek objednatele řádně a včas

   - **převzít plně funkční EDR řešení a zaplatit za něj zhotoviteli** dohodnutou cenu dle čl. IV této smlouvy,
   - **platit za technickou podporu** dohodnutou cenu dle čl. IV. této smlouvy.

Zhotovitel je vázán svou nabídkou předloženou v rámci zadávacího řízení k veřejné zakázce malého rozsahu na dodávku s názvem „Systém pro ochranu koncových stanic a serverů – EDR“.

II.
Financování předmětu smlouvy

1. Zhotovitel bere na vědomí, že předmět smlouvy bude spolufinancován z Integrovaného regionálního operačního programu (IROP) 2021 – 2027 Ministerstva pro místní rozvoj ČR v rámci výzvy č. 10 eGovernment a kybernetická bezpečnost.
   Název projektu: Posílení kybernetické bezpečnosti IS ÚMČ Praha 12
   Registrační číslo projektu: CZ.06.01.01/00/22_010/0002965

III.
Doba trvání a místo plnění předmětu smlouvy

1. Místem plnění je sídlo objednatele.
2. Zhotovitel se zavazuje
   - okamžikem nabytí účinnosti smlouvy zahájit realizaci díla, tj. dodávku EDR řešení,
   - ve lhůtě 45 dnů od zahájení dokončit dílo do stavu plně funkčního EDR řešení způsobilého k převzetí objednatelem bez výhrad.
3. Zhotovitel se zavazuje poskytovat technickou podporu po dobu 36 měsíců ode dne převzetí díla objednatelem bez výhrad.

IV.
Cena díla a platební podmínky

1. Cena za plnění dle čl. I. bod 1.1. této smlouvy je sjednána následovně:

Položka	**cena bez DPH**	**cena vč. DPH**
Dodávka systému EDR pro ochranu 300 koncových stanic a 50 virtuálních serverů včetně instalace a implementace	**990.020 Kč**	**1.197.924 Kč**
Poskytování technické podpory na období 36 měsíců	**199.980 Kč**	**241.976 Kč**
CELKOVÁ CENA	**1.190.000 Kč**	**1.439.900 Kč**

2. Cena za dodávku je splatná na základě daňového dokladu – faktury, který zhotovitel vystaví do čtrnácti (14) kalendářních dnů od převzetí díla objednatelem. Povinnou přílohou faktury je akceptační protokol o předání a převzetí dle čl. V. této smlouvy,
3. Cena za poskytování technické podpory je sjednána za 36 měsíců, fakturována bude objednatelem po částech, vždy na následující kalendářní rok, fakturou splatnou nejpozději 15.12. daného kalendářního roku.
4. Daňový doklad/faktura musí obsahovat veškeré náležitosti dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a informace povinně uváděné na obchodních listinách na základě § 435 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „*občanský zákoník*“). Faktury budou vystaveny se splatností třicet (30) dní ode dne jejich doručení objednateli. Faktura musí být označena názvem veřejné zakázky předcházející uzavření této smlouvy – „*Systém pro ochranu koncových stanic a serverů – EDR*“ a dále registračním číslem projektu: CZ.06.01.01/00/22_010/0002965. Faktury budou zasílány na adresu objednatele v listinné podobě (ve dvou vyhotoveních), případně elektronicky prostřednictvím datové schránky. Za den úhrady dané faktury bude považován den odepsání fakturované částky z účtu objednatele.
5. Objednatel vrátí zhotoviteli bez zaplacení fakturu, která neobsahuje náležitosti uvedené v předchozích ustanoveních tohoto článku nebo jiné náležitosti vyžadované příslušnými právními předpisy. Vrácením faktury se přerušuje doba splatnosti a nová doba počíná běžet znovu ode dne doručení opravené faktury nebo nově vyhotovené faktury.
6. Daň z přidané hodnoty bude účtována v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, v sazbě platné ke dni uskutečnění zdanitelného plnění.

Článek V.
Předání a převzetí předmětu plnění

1. Převzetí díla včetně související dokumentace bude probíhat na základě akceptační procedury podrobněji specifikované v následujících bodech, která zahrnuje

- provedení akceptačních testů, tj. porovnání skutečných vlastností EDR řešení s technickou specifikací dle přílohy č. 1 této smlouvy,

- v případě jejich úspěšného splnění podepsání akceptačního protokolu oprávněnými zástupci obou smluvních stran, kterými jsou

za **zhotovitele:** [redacted] a

za **objednatele**: [redacted] odbor informačních technologií, ÚMČ Praha 12, tel: [redacted]

2. Objednatel do deseti (10) pracovních dní ode dne provedení akceptačních testů

   - podepíše protokol o provedení akceptačních testů a vyznačí v něm

     - „převzato“ - dílo při akceptačních testech nevykázalo vady, odpovídá technické specifikaci dle přílohy č. 1 této smlouvy a je tedy způsobilé k převzetí objednatelem, který převzetí potvrdí podpisem protokolu, akceptační procedura končí;

     - „převzato s výhradou“ - dílo vykazuje vady, které nebrání jeho převzetí, objednatel do protokolu poskytne zhotoviteli přiměřenou lhůtu k odstranění vad, akceptační procedura se zopakuje, jen pokud to vyhodnotí jako nezbytné zástupce objednatele;

     - „převzetí odmítnuto“ – dílo není v souladu s technickou specifikací dle přílohy č. 1 této smlouvy; objednatel do protokolu poskytne zhotoviteli přiměřenou lhůtu k odstranění vad, akceptační procedura se zopakuje;

   nebo

   - oznámí e-mailem zhotoviteli důvody, které brání převzetí díla.

3. Podpisem akceptačního protokolu s vyznačením „převzato“ nebo odstraněním vad v případě akceptačního protokolu s vyznačením „převzato s výhradou“ je akceptační procedura dokončena.
4. Dokončení akceptační procedury opravňuje zhotovitele k fakturaci.
5. Dnem převzetí díla objednatelem a tedy i dne přechodu vlastnického práva a nebezpečí škody na objednatele je den podpisu akceptačního protokolu.
6. Podpisem akceptačního protokolu není dotčeno právo objednatele domáhat se práv z jakýchkoliv následně zjištěných vad díla.
7. V případě, že zhotovitel dodá objednateli dílo, o němž věděl nebo mohl vědět, že nesplňuje technické požadavky objednatele, je objednatel oprávněn uplatnit smluvní pokutu dle čl. VIII. této smlouvy.

Článek VI.
Práva a povinnosti zhotovitele

1. Zhotovitel se zavazuje spolupracovat s objednatelem a poskytovat mu veškerou nutnou součinnost potřebnou pro řádné plnění předmětu této smlouvy.
2. Zhotovitel se zavazuje písemně nebo prostřednictvím e-mailu informovat objednatele o veškerých skutečnostech, které jsou nebo mohou být důležité pro plnění předmětu této smlouvy, zejména ho informovat o požadavcích na součinnost.
3. Zhotovitel se zavazuje dodat dílo v množství, jakosti a provedení, jež určuje tato smlouva.
4. Zhotovitel se zavazuje k plnění této smlouvy využít pouze ty technické poradce, jejichž seznam tvoří přílohu č. 2 této smlouvy.

5. Jakékoliv změny či obměny technických poradců, jejichž prostřednictvím prokazoval zhotovitel splnění technické kvalifikace v rámci zadávacího řízení, jsou možné jen za předchozího souhlasu objednatele a pouze za předpokladu, že technický poradce, který má nahradit původního technického poradce, disponuje stejnou nebo vyšší kvalifikací (technickou kvalifikací prokazovanou v zadávacím řízení původním technickým poradcem), jako technický poradce původní.
6. Zhotovitel se zavazuje uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů nejméně do 31. 12. 2035.

   Dokumenty se uchovávají ve formě originálů nebo kopií originálů, na běžných nosičích dat, v elektronické verzi originálních dokladů nebo dokladů existujících pouze v elektronické podobě.

   Pokud doklady existují pouze v elektronické podobě, musí používané počítačové systémy splňovat uznávané bezpečnostní normy, které zajistí, že uchovávané doklady splňují požadavky vnitrostátních právních předpisů a jsou dostatečně spolehlivé pro účely auditu.

   U dokumentů uchovávaných v digitální podobě je třeba zajistit, aby zápis byl proveden ve formátu, který zaručí jeho neměnnost. Pokud to zajistit nelze, musí být dokumenty převedeny do analogové formy a opatřeny náležitostmi originálu.
7. Zhotovitel se zavazuje nejméně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

Článek VII.
Práva a povinnosti objednatele

1. Objednatel se zavazuje poskytnout zhotoviteli součinnost pro řádné plnění předmětu této smlouvy. Rozsah součinnosti dle přílohy č. 1 této smlouvy je pouze předpokládaný rozsah, skutečný rozsah vyplývá z povahy díla a náročnosti instalace a implementace.
2. Pokud objednatel neposkytne zhotoviteli potřebnou součinnost, má zhotovitel právo na prodloužení lhůty k plnění o čas, po který nemohl plnit své závazky.

Článek VIII.
Licenční ujednání

1. V případě, že při plnění předmětu smlouvy vzniknou výstupy zhotovitele, které by naplňovaly znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), objednatel bez dalšího nabývá nevýhradní právo užít takovéto dílo, a to k jakémukoliv účelu a rozsahu (dále jen „**licence**“). Zhotovitel se zavazuje bez zbytečného odkladu informovat objednatele o vzniku takových práv k duševnímu vlastnictví.
2. Zhotovitel není oprávněn udělení licence vypovědět, přičemž účinnost licence trvá i po skončení účinnosti této Smlouvy.

3. Licence se vztahuje také na všechny nové verze, aktualizované verze, i na úpravy a překlady autorského díla, pořízené objednatelem.
4. Cena za poskytnutí licence je zahrnuta v celkové ceně plnění dle této smlouvy.
5. Tato licenční ujednání jsou sjednaná na dobu trvání autorských práv zhotovitele.

Článek IX.
Důvěrnost informací

1. Zhotovitel se zavazuje během plnění smlouvy i po uplynutí doby, na kterou je smlouva uzavřena, zachovávat mlčenlivost o všech skutečnostech, o kterých se při plnění předmětu smlouvy dozví, a nakládat s nimi jako s důvěrnými (s výjimkou informací, které již byly veřejně publikované).
2. Zhotovitel je oprávněn zpracovávat pouze osobní údaje nezbytné pro splnění předmětu této smlouvy, zejména jméno, příjmení, e-mailovou adresu a telefonní číslo osob objednatele, a to na základě doložených pokynů objednatele (dále jen „údaje“).
3. Zhotovitel se zavazuje, že pokud v souvislosti s realizací této smlouvy při plnění svých povinností přijdou jeho pověření zaměstnanci do styku s údaji ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“), učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož aby i jinak GDPR porušil. Zhotovitel nese plnou odpovědnost za případné porušení GDPR z jeho strany. Zhotovitel nezapojí do zpracování údajů žádné další osoby mimo svých pověřených zaměstnanců a zajistí, aby se jeho pověření zaměstnanci, oprávnění zpracovávat údaje, zavázali k mlčenlivosti.
4. S ohledem na opatření proti neoprávněnému nebo nahodilému přístupu k údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům a zpracování, o nichž je řeč v předchozím odstavci, se zhotovitel zavazuje přijmout opatření vyjmenovaná v čl. 32. GDPR, přičemž zároveň přihlédne ke stavu techniky, nákladům na provedení, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.
5. Zhotovitel bude objednateli bez zbytečného odkladu nápomocen při plnění povinností objednatele, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení údajů dozorovému úřadu dle čl. 33 GDPR, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 GDPR, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 GDPR a povinnosti provádět předchozí konzultace dle čl. 36 GDPR, a že za tímto účelem zhotovitel zajistí nebo přijme vhodná technická a organizační opatření dle předchozího odstavce, o kterých ihned informuje objednatele.
6. Zhotovitel není oprávněn jakkoliv využít informace, údaje a dokumentaci, která mu byla zpřístupněna v souvislosti s prováděním díla, ve prospěch svůj nebo třetí osoby. Zhotovitel je povinen dodržovat tyto povinnosti také po ukončení smluvního vztahu mezi objednatelem a zhotovitelem až do doby, kdy bude těchto povinností zproštěn.
7. Zhotovitel poskytne objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené příslušnými právními předpisy.

8. Zhotovitel umožní kontroly, audity či inspekce prováděné objednatelem nebo jiným příslušným orgánem dle příslušných právních předpisů.
9. Zhotovitel poskytne bez zbytečného odkladu nebo ve lhůtě, kterou stanoví objednatel, součinnost potřebnou pro plnění zákonných povinností objednatele spojených ochranou osobních údajů, jejich zpracováním a s plněním smlouvy o zpracování osobních údajů.
10. Zhotovitel je povinen provést likvidaci údajů neprodleně po převzetí a odsouhlasení poskytovaného plnění objednatelem.

Článek X.
Záruční podmínky, sankce

1. Odpovědnost za vady a nároky z ní vyplývající se řídí příslušnými ustanoveními občanského zákoníku, zejména ustanovením § 2099 a souvisejícími.
2. Zhotovitel poskytuje na dílo záruku po dobu 36 měsíců od převzetí díla objednatelem. Zárukou se zhotovitel zavazuje, že plnění bude po záruční dobu způsobilé k použití pro obvyklý účel nebo že si zachová obvyklé vlastnosti.
3. Při nedodržení termínu splatnosti řádně vystavené faktury/daňového dokladu objednatelem je zhotovitel, který řádně splnil své povinnosti, oprávněn požadovat zaplacení úroku z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroku z prodlení a nákladů spojených s uplatněním pohledávky, ve znění pozdějších předpisů.
4. V případě prodlení zhotovitele s provedením díla ve lhůtě dle čl. III., bod 1 má objednatel právo uplatnit vůči zhotoviteli smluvní pokutu ve výši 10.000,- Kč za každý i započatý kalendářní den prodlení. Toto ustanovení se nevztahuje na plnění povinností objednatele v rámci čl. III. bod 3 (poskytování technické podpory).
5. Pokud se prokáže, že zhotovitel nepravdivě uvedl rozsah skutečných vlastností díla dle čl. I., bod 1.1. se specifikací dle této smlouvy, zejména její přílohy č. 1 nebo nepravdivě uvedl rozsah požadovaných licenčních oprávnění a na základě této skutečnosti dojde k nepřevzetí díla dle čl. V. smlouvy a uplynutí lhůty stanovené na realizaci díla dle čl. III smlouvy, je objednatel oprávněn účtovat pokutu ve výši 2.000.000,- Kč, přičemž toto porušení smlouvy bude zároveň považováno za její podstatné porušení a objednateli vedle práva na smluvní pokutu vznikne též právo na odstoupení od smlouvy.
6. V případě nedodržení lhůt dle článku XI. bodu 1. této smlouvy zhotovitelem má objednatel nárok na smluvní pokutu ve výši 10.000,- Kč za každý započatý pracovní den prodlení (tj. prodlení v případě nezahájení řešení do jednoho (1) pracovního dne po zadání incidentu).
7. Smluvní pokuty jsou splatné ve lhůtě sedmi (7) dnů od doručení písemné výzvy objednatele k úhradě.
8. Objednatel má právo na náhradu škody v plné výši vzniklé porušením povinnosti, ke kterému se smluvní pokuta vztahuje.
9. Zaplacení smluvní pokuty nezbavuje zhotovitele povinnosti splnit závazek utvrzený smluvní pokutou.

Článek XI.
Technická podpora

1. Zhotovitel se zavazuje poskytovat službu technické podpory v rozsahu dle této smlouvy, zejména její přílohy č. 1, nejméně však v režimu 5 dní x 8 hodin / týden (pondělí – pátek v čase 8:00 – 16:00), a zahájit řešení vady, tj. neplánovaného přerušení fungování EDR řešení, omezení kvality jeho fungování, jakákoliv prokazatelná nefunkčnost EDR řešení nebo některé z jeho základních funkcí či provozních funkcionalit, nejpozději s odezvou do osmi (8) hodin a zahájení řešení do jednoho (1) pracovního dne po zadání incidentu dle postupu uvedeného níže.
2. Zhotovitel se zavazuje v rámci technické podpory pravidelně informovat objednatele o dostupnosti nové verze softwaru, jež je součástí předmětu díla, upozornit na potenciální chyby a rizika, jsou-li známy, a na výzvu objednatele novou verzi implementovat.
3. Objednatel se zavazuje informovat zhotovitele o incidentech bez zbytečného odkladu poté, kdy incident zjistil, na níže uvedené kontakty zhotovitele: support.altepro.cz, tel.: +420 840 11 22 33, e-mail: support@altepro.cz.
4. V případě, že je v příloze č. 1 uveden jiný rozsah technické podpory, platí rozsah pro objednatele příznivější.

Článek XII.
Náhrada škody

1. Zhotovitel zodpovídá v plné výši za veškeré škody způsobené objednateli porušením této smlouvy či právních předpisů, za škody vzniklé v důsledku vadného plnění a vůči objednateli i třetím osobám za škody způsobené protiprávním činem.
2. Povinnosti k náhradě škody se zhotovitel zprostí, pokud prokáže existenci okolností dle § 2913 odst. 2 občanského zákoníku.
3. Zhotovitel před podpisem této smlouvy předal objednateli kopii pojistné smlouvy (pojistky nebo pojistného certifikátu), jejímž předmětem je pojištění odpovědnosti za škodu způsobenou v souvislosti s prováděním jeho podnikatelské činnosti ve výši horní hranice pojistného plnění minimálně 2.000.000,- Kč na jednu pojistnou událost. Zhotovitel je povinen mít v účinnosti pojistnou smlouvu po celou dobu poskytování předmětu plnění a kdykoliv na požádání objednatele osvědčit její trvání.

Článek XIII.
Trvání a ukončení smlouvy

1. Tato smlouva se uzavírá na dobu určitou. Nabývá účinnosti jejím podpisem oprávněnými zástupci smluvních stran a končí uplynutím 36 měsíců ode dne následujícího po protokolárním převzetí díla objednatelem.
2. Smluvní vztah lze ukončit písemnou dohodou smluvních stran nebo odstoupením v souladu s občanským zákoníkem. Objednatel je oprávněn tuto smlouvu vypovědět i bez udání důvodu s výpovědní dobou šest (6) měsíců. Zhotovitel není oprávněn tuto smlouvu vypovědět.
3. Smluvní strany jsou oprávněny odstoupit od smlouvy z důvodů uvedených v této smlouvě a dále z důvodů uvedených v zákoně, zejména v případě podstatného porušení smlouvy.

4. Podstatným porušením smlouvy zhotovitelem, které je důvodem pro odstoupení od smlouvy ze strany objednatele, je:

   - prodlení se zhotovením díla ve sjednané lhůtě dle čl. III. této smlouvy;

   - dodání EDR řešení, které není plně funkční ve smyslu potřeb objednatele nebo které není v souladu s technickou specifikací dle zadávací dokumentace k veřejné zakázce, jejímž výsledkem je tato smlouva.

   - porušení povinností zhotovitele, které nebude odstraněno ani do 30 kalendářních dní od doručení písemné výzvy objednatele dnů

5. Podstatným porušením smlouvy objednatelem, které je důvodem pro odstoupení smlouvy ze strany zhotovitele, je

   - prodlení objednatele s úhradou faktury/daňového dokladu o více jak 30 kalendářních dní od doručení písemné výzvy zhotovitele k zajištění nápravy; nárok na úrok z prodlení není tímto dotčen.

6. V případě odstoupení od smlouvy objednatelem pro podstatné porušení smlouvy zhotovitelem:

   - nemá zhotovitel nárok na jakoukoliv náhradu nákladů, které mu vznikly za dobu trvání smlouvy,

   - má objednatel (kromě jiného) nárok na náhradu škody, na náhradu prokazatelných nákladů, které mu vzniknou v souvislosti se zajištěním náhradního plnění a dále na vrácení poměrně části ceny za nevyčerpané plnění; nároky z vadného plnění nejsou dotčeny.

7. Odstoupení od této smlouvy musí být písemné a musí obsahovat odkaz na ustanovení této smlouvy, které zakládá oprávnění od smlouvy odstoupit.

8. Smluvní vztah skončí dnem doručení oznámení o odstoupení od smlouvy druhé smluvní straně, nebo dnem uvedeným v oznámení.

9. Odstoupení od této smlouvy či jiné ukončení smluvního vztahu založeného touto smlouvou se nedotýká práva na zaplacení smluvní pokuty nebo úroku z prodlení, pokud již dospěl, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat strany i po odstoupení od smlouvy.

Článek XIV.
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem jejího uveřejnění dle zákona č. 340/2015 Sb., o registru smluv. Uveřejnění zajistí objednatel.

2. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla veřejně přístupná v celém rozsahu.

3. Změny a doplňky této smlouvy lze provést pouze formou písemných číslovaných dodatků.

4. V případě, že by se některé ustanovení této smlouvy stalo zdánlivým, neplatným či neúčinným, nezpůsobuje tato skutečnost neplatnost ani neúčinnost ostatních částí smlouvy. Smluvní strany se ho zavazují po vzájemné dohodě nahradit jiným ustanovením, blížícím se svým obsahem nejvíce účelu zdánlivého, neplatného či neúčinného ustanovení.

5. Smluvní vztahy výslovně neupravené touto smlouvou, nebo upravené jen částečně, se řídí příslušnými ustanoveními občanského zákoníku, popř. autorského zákona.
6. Tato smlouva je vyhotovena v jednom (1) vyhotovení v českém jazyce s platností originálu s elektronickými podpisy obou smluvních stran.
7. Nedílnou součástí této smlouvy jsou její přílohy:

   příloha č. 1 – Technická dokumentace – podrobný popis díla a specifikace věcí k provedení díla a dílčích činností zhotovitele

   příloha č. 2 – Seznam technických poradců

Tato smlouva byla schválena Radou městské části Praha 12 usnesením č. R-93-005-24 dne 20. 9. 2024.

Za objednatele:	Za zhotovitele:
V Praze dne	V Praze dne .....
.....	.....
Ing. Vojtěch Kos, MBA starosta	Vladimír Fiala, jednající na základě plné moci

Příloha č. 1 - Technická dokumentace – podrobný popis díla a specifikace věcí k provedení díla a dílčích činností zhotovitele

1) Specifikace technických údajů (výrobce, typ licence…) včetně technického popisu:

Nabízené řešení je od výrobce Trend Micro Inc. Předmětem plnění je nákup EDR/XDR systému a to v níže uvedeném počtu licencí a požadované specifikace.

- Licence pro koncové stanice a servery 350 ks
- Tzv. Sandbox submisision 100 kreditů
- ASMR modul na zařízení 350 ks
- Vše na dobu 36 měsíců

Počet licencí	Part number výrobce	Popis výrobce
350	VO01191189	Trend Vision One - Endpoint Security (Essentials), New, Government, 251-500 License, 36 months
100	VO01158935	Trend Micro Vision One Credits, Government, 1-999999999 License, 36 months
350	VO01202204	Trend Vision One Attack Surface Risk Management for on-premise desktops and servers, New, Government, 251-500 License, 36 months

Stručný popis řešení

Vision One Endpoint Security

Ochrana koncových stanic, desktopů a serverů, včetně XDR.

Možnost nasazení v různých variantách a jejich libovolných kombinacích, integrovaných do jedné konzole:

- XDR senzor, pouze EDR komponenta, která může běžet samostatně.
- Standard Endpoint Protection, ochrana koncových stanic a serverů na platformě Windows a MacOS, se zaměřením na desktopy.
- Server & Workload Protection, ochrana koncových stanic a serverů na platformě Windows, Linux, AIX atd. s pokročilou funkcionalitou zaměřenou na servery.

Trend Vision OneTM - Endpoint Security je řešení zabezpečení koncových bodů, které je určeno pro koncové body, servery a cloud a integruje pokročilou ochranu proti hrozbám,

EDR/XDR a zpravodajství o hrozbách. Tato platforma pomáhá zefektivnit IT/bezpečnostní operace, snížit složitost a dosáhnout optimálních výsledků zabezpečení v lokálních, cloudových, multicloudových a hybridních prostředích.

Jako součást Trend Vision OneTM - moderní, cloudové platformy kybernetické bezpečnosti s nejširší sadou nativních řešení doplněných o integraci s třetími stranami - propojuje zabezpečení koncových bodů s dalšími produkty pro ochranu, threat inteligence, SIEM, orchestraci, řízení rizik a další. Zabezpečení koncových bodů podporuje různorodá hybridní IT prostředí, pomáhá při automatizaci a orchestraci pracovních postupů a poskytuje odborné služby kybernetické bezpečnosti, takže umožňuje rychleji zastavit protivníky a převzít kontrolu nad kybernetickými riziky.

Vision One Attack Surface Risk Management

Nástroj pro hodnocení a sledování rizik. Automaticky neustále průběžně monitoruje riziko detekovaných zařízení v infrastruktuře, všech uživatelů a také celkové riziko organizace.

ASRM je řešení nové generace, které přináší vylepšené, proaktivní zabezpečení od SecOps až po vedení společnosti. Systém ASRM, podpořený špičkovým výzkumem v oboru, umožňuje vedoucím pracovníkům a týmům v oblasti zabezpečení zjišťovat a kontextuálně vyhodnocovat celkové riziko organizace. Kromě toho umožňuje využívat pokročilé modely AI a ML, které vytvářejí nápravná doporučení, jež pomáhají proaktivně zmírňovat rizika a zmenšovat plochu útoku.

Zobrazení přístrojového panelu ASRM v aplikaci Trend Vision OneTM, doplněné o skóre organizačního rizika.

Využití ASRM umožňuje:

- Rychlé průběžné odhalování útoků.
- Hodnocení rizik v reálném čase.
- Prioritizované poznatky o rizicích s doporučeními.
- Proaktivní nápravu a správu rizik.
- Dashboardy a reporty.

Pro kompletní popis produktu jsou k dispozici datasheety výrobce:

1. Endpoint security: www.trendmicro.com/en_us/business/products/endpoint-security.html?modal=s7b-card-btn-endpoint-sec-ds-1a8e15
2. ASRM: www.trendmicro.com/en_us/business/products/detection-response/attack-surface-management.html?modal=s8a-card-btn-asrm-ds-5da2c7

Verifikační tabulka řešení

Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno) a požadované funkce	Splněno ANO/NE	Stručný popis plnění
1. Konzole pro centrální správu řešení:		
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí	ANO	Výrobce provozuje konzoli v cloudu AWS a Azure. Zajišťuje plně její provoz a respektuje potřebné regulatorní povinnosti.
Konzole pro centrální správu je kompletně multi-tenantní	ANO	Cloudová konzole je multitenantní a lze se mezi tenanty přepínat.
Základní vlastnosti		
Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu	ANO	Lze buď pomocí secure gateway (virtuální appliance) a nebo přepnutím jednoho endpointu do relay modu.
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem	ANO	
Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce	ANO	Nabízená centrální konzole má veřejné API, které lze pro integraci použít. Případně existuje spousta již předpřipravených integrací – také spravovaných v konzoli.
Úlohy správy bezpečnosti		
Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.	ANO	Integrace se provádí s využitím onprem virtualní appliance, která propojí cloud s onprem AD.
Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery	ANO	Existuje mnoho metod, jak tohoto docílit. Součástí ASRM subscripce (Attack Surface Risk Management) je velmi mocný nástroj, který mimojiné dělá asset inventory na základě síťové komunikace, kterou vidí zařízení pod správou. Přiřazuje k assetum risk score a eviduje mnoho dalších informací. Další možnost je podporovaná integrace s nessus scanem apod.
Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity	ANO	
Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy	ANO	Ano, požadované chování jsme schopni zajistit pomocí powershell skriptu, který se spustí na endpointu s agentem z administrátorské konzole centrální správy.netw
Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy	ANO	Powershell a nebo bash scriptem, který lze spustit z konzole.
Centralizované místo pro záznam všech úloh	ANO	Všechny úlohy jsou zaznamenané, včetně autora a logu celé session.
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)	ANO	
Reportování		

Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě	ANO	Lze nastavit velmi flexibilně. Existuje spousta šablon, které si uživatel může upravit a nastavit jim interval, formát, doplnit firemní logo apod.
Možnost zasílání vygenerovaných reportů e-mailem	ANO	Na emaily uživatelů konzole a nebo i na libovolné další email adresy.
Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv	ANO	
Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen	ANO	Za předpokladu, že je funkční propoj na service gateway.
Karanténa		
Vzdálená obnova či smazání souboru v karanténě	ANO	Z centrálního adresáře karantény umístěného v cloudu.
Možnost automaticky přidat soubor do výjimky při obnově z karantény	ANO	Při obnově souboru z karantény lze zaškrtnout, že z něj je třeba vytvořit výjimku, která bude následně
Uživatelé		
Více předdefinovaných rolí:		
Root, administrátor, reportér		Master admin, operator, auditor, senior analyst, analyst, endpoint administrator, email administrator
1. Root: spravuje komponenty řešení	ANO	Odpovídá roli „Master administrator“
2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení	ANO	Odpovídá roli „Endpoint administrator“
3. Reportér: spravuje a vytváří reporty	ANO	Lze nadefinovat jako custom roli, připadne použít auditora.
Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)	ANO	
Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat	ANO	Vše se řeší v definice ROLE.
Logy		
Zaznamenávání uživatelských akcí	ANO	Vše je v audit logu
Detailní log pro každou akci	ANO	
Komplexní vyhledávání v logách	ANO	
Správa a instalace ochrany		
Instalace může být provedena několika způsoby, alespoň:		Poznámka: Máme za sebou instalace tisíců endpointů a nesetkali jsme se s potřebou instalovat vzdáleně z konzole.
1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován	ANO	Balíček je generován přímo v tenantu zákazníka.
2. Instalace vzdáleně přímo z konzole správy	ANO	Stejný komentář jako u otázky v sekci: Úlohy správy bezpečnosti
3. Distribuce instalačního balíčku pomocí GPO či SCCM	ANO	
Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN	ANO	Dalo by se řešit custom akci např s pomocí powershell skriptu, který se připojí na sousední koncovou stanici a klienta nainstaluje. Ale rozhodně to není v dnešní době uvažované řešení a nejde o uživatelsky přívětivé řešení.
Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou	ANO	

Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci	ANO	Konzole je v tomto velice flexibilní.
Konzole správy obsahuje detailní informace o chráněných strojích	ANO	V základu obsahuje řadu užitečných informací. V případě ASRM funkce, se toto ještě výrazně rozšíří – risk score, instalované aplikace, evidované CVEčka, uživatelské účty, asset graph – kam všude přistupuje a mnoho dalšího.
Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice	ANO	Vše se řeší s centrální konzole, tedy včetně kompletní správy ochrany koncových stanic.
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou	ANO	Samozřejmě, typicky přes profily, které následně aplikujeme na jeden, více či na všechny koncové stanice.
Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat	ANO	
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy	ANO	Balíčky navíc můžou být rovnou zařazené do skupiny, mohou mít nastavenou proxy apod.
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)	ANO	Lze vypnout notifikaci uživatele a tím potřebu jeho interakce vyloučit.
Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body	ANO	
Možnost spustit Network discovery z kteréhokoli již instalovaného klienta	ANO	Ano, potvrzujeme. Endpointy detekují díky ASRM funkcionalitě automaticky IP adresy, se kterými navážou síťovou komunikaci (včetně zařízení mimo AD a zařízení BYOD). Konzole pak zobrazuje přehled všech zařízeních v síti – tedy jak endpointů chráněných agentem, tak endpointů bez agenta.
1. Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):		
Podpora operačních systémů:		
Windows 11	ANO	
Windows 10 1507 a vyšší	ANO	
Windows Embedded POSReady 7	ANO	
Windows Server 2022	ANO	
Windows Server 2022 Core	ANO	
Windows Server 2019	ANO	
Windows Server 2019 Core	ANO	
Windows Server 2016	ANO	
Windows Server 2016 Core	ANO	
Windows Server 2012 R2	ANO	
Windows Server 2012	ANO	
Windows Server 2008 R2	ANO	
Ubuntu 16.04 LTS a vyšší	ANO	
Red Hat Enterprise Linux 7xx	ANO	
CentOS 7.0 a vyšší	ANO	

SUSE Linux Enterprise Server 12 SP4 a vyšší	ANO	
Fedora 31-36	ANO	
Debian 9.0-11.0	ANO	
Oracle Linux 7.x-8.x	ANO	
Mac OS X Sierra (10.12) a vyšší	ANO	
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Automatické skenování paměti procesů v reálném čase	ANO	
Detekce na základě virových definicí (tzn. signatur)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení	ANO	
Detekce 0-day útoků na základě odhalování anomálního chování	ANO	
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení	ANO	
Detekce 0-day bezsouborových útoků	ANO	
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)	ANO	
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností	ANO	Součástí ASRM
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je toto CVE uvedeno	ANO	
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP	ANO	Ano, EPP i EDR senzor jsou provozovaný v rámci jedné aplikace.
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy	ANO	Buď automatickou response akcí a nebo akcí vyvolanou uživatelem konzole (s dostatečnými oprávněními).
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.	ANO	NEJEN v době incidentu, ale po celou dobu. Bez toho je EDR mnohdy slepé – neboť některé události lze spojit s aktivitou útočníka až zpětně.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.	ANO	Samozřejmě z pohledu endpointu. Lze případně obohatit síťovou sondou, která je plně integrovaná do celého řešení.
Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem	ANO	Navíc lze definovat vlastní IOC.
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku	ANO	Samozřejmě, navíc lze vygenerovat execution tree i na události, které nejsou rozpoznány jako útok. Toto se ukazuje jako velmi užitečná funkce.
Řešení umožňuje analýzu vektoru útoku	ANO	

Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování	ANO	NEJEN v době incidentu. Víceméně stejná odpověď jako o pár otázek výše.
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)	ANO	Hledat lze na základě jakýchkoliv posbíraných dat s pomocí Search funkce a šikovného dotazovacího jazyka. Lze jít až na úroveň dotazovaných URL, hashi, procesů, uživatelů, IP adres apod.
Řešení umožňuje vzdálené připojení na příkazové řádek koncového bodu (Powershell, Zshell, Bash/výchozí CLI v Linux)	ANO	Řešení využívá pro připojení vlastní shell, který nabízí některé užitečné funkce (např memorydump). V případě potřeby volat konkrétní powershell,bash apod příkazy, lze to dělat pomocí skriptu, který na koncovou stanici zavoláme z konzole.
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní	ANO	Data o bezpečnostních incidentech jsou uloženy i déle, co je klíčové je detailní kompletní telemetrie – ta je uložena v základu 30 dní a lze prodloužit až na rok za poplatek.
Možnost skenovat archivy	ANO	Včetně vícenásobně komprimovaných souborů.
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID	ANO	
Možnost rozšíření na XDR - sonda síťového provozu	ANO	Řešení nazvané: Network Security
Možnost rozšíření na XDR - sonda do AD, Azure AD, MS Intune	ANO	Součástí : Cloud
Možnost rozšíření na XDR - sonda do Office365/Microsoft365	ANO	Součástí : Email and Collaboration security
Možnost rozšíření na XDR – sonda do Azure	ANO	Součástí : Cloud app
Možnost rozšíření na XDR – sonda do AWS	ANO	Součástí : Cloud app
Možnost rozšíření na XDR – sonda do Google Workspace	ANO	Součástí : Email and Collaboration security
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)	ANO	Ano, vše je součástí Vision One – centrální konzole.
Karanténa		
Možnost obnovy souboru do originální či do nově zadané lokality	ANO	
Kontrola přístupu k internetu		
Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)	ANO	Wildcards lze použít libovolně v URL
1. Ochrana virtualizovaných koncových bodů (Windows, Linux)		Řešení se neliší od fyzických koncových bodů. Pouze pokud by došlo k nasazení na VDI, tak je třeba řešit některé věci trošku okolo spotřeby licencí apod.
Podpora operačních systémů:		
Windows 11	ANO	
Windows 10 1507 a vyšší	ANO	
Windows Embedded Compact 7	ANO	
Windows Server 2022	ANO	
Windows Server 2022 Core	ANO	

Windows Server 2019	ANO	
Windows Server 2019 Core	ANO	
Windows Server 2016	ANO	
Windows Server 2016 Core	ANO	
Windows Server 2012 R2	ANO	
Windows Server 2012	ANO	
Windows Small Business Server 2011	ANO	
Windows Server 2008 R2	ANO	
Ubuntu 16.04 LTS a vyšší	ANO	
Red Hat Enterprise Linux 7xx	ANO	
CentOS 7.0 a vyšší	ANO	
SUSE Linux Enterprise Server 12 SP4 a vyšší	ANO	
Fedora 31-36	ANO	
Debian 9.0-11.0	ANO	
Oracle Linux 7.x-8.x	ANO	
Mac OS X Sierra (10.12) a vyšší	ANO	
Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna	ANO	
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Detekce na základě virových definicí (tzn. signatur)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Automatické skenování paměti procesů v reálném čase (včetně ochrany proti 0-day útokům)	ANO	
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení	ANO	
Detekce 0-day útoků na základě odhalování anomálního chování	ANO	
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení	ANO	
Detekce 0-day bezsouborových útoků	ANO	
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)	ANO	
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy	ANO	
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.	ANO	

Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.	ANO	
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku	ANO	
Řešení umožňuje analýzu vektoru útoku	ANO	
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování	ANO	
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)	ANO	
Řešení umožňuje vzdálené připojení na příkazové řádek koncového bodu (Powershell, Zshell, Bash/výchozí CLI v Linux)	ANO	
Možnost skenovat archivy	ANO	
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID	ANO	
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)	ANO	
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní	ANO	
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)	ANO	
Dodavatel prohlašuje, že neobchoduje se sankcionovaným zbožím, které se nachází v Rusku nebo Bělorusku či z Ruska nebo Běloruska pochází a nenabízí takové zboží v rámci plnění veřejných zakázek.	ANO	

2) <u>Rozsah a způsob poskytování technické podpory:</u>

Objednatel bude požadované služby využívat prostřednictvím helpdesku Zhotovitele. Zhotovitel bude poskytovat Objednateli podporu a konzultace k dotčeným systémům na těchto komunikačních rozhraních:

- e-mail: support@altepro.cz
- web: support.altepro.cz
- telefon: 840 11 22 33

Zajištění centrální hotline pro hlášení závad a požadavků:

- Telefonická hotline (dostupnost 24x7)
- Webový portál (dostupnost 24x7)
- E-mailová adresa (dostupnost 24x7)

Dále jsou k dispozici telefonní kontakty technických poradců v požadovaném čase.

Rozsah a poskytování technické podpory odpovídá plně znění čl. XI. a také specifikacím v Technické části Smlouvy.

3) Předpokládaný rozsah součinnosti objednatele

Součinnost Objednatele se předpokládá běžná, tedy součinnost na úvodní a pracovní schůzky, školení, konzultační schůzky v době plnění Smlouvy. Dále součinnost při řešení bezpečnostních nebo technických problémů.

4) Předpokládaný termín dodávky

Nejzazší termín dodávky je do 45 dní od účinnosti Smlouvy.

Součástí realizace díla je:

a) Instalace a implementace – činnosti související s iniciální implementací a integrací do stávající infrastruktury objednatele zahrnují (rozsah bude odpovídat této technické specifikaci a detailní zadání bude upřesněno před samotnou implementací):

- fyzická instalace a zprovoznění EDR řešení tak, aby plnilo svůj účel, tedy komplexní ochranu koncových stanic a serverů objednatele (níže uvedeným požadavkům a best practise výrobce);
- integrace, konfigurace a propojení s prvky objednatele;
- vytvoření dokumentace;
- seznámení administrátorů se správou a konfigurací dodaného systému minimálně v rozsahu minimálně 3MD:
    - seznámení se systémem, způsoby obsluhy a konfigurace (předpokládá se účast 5 pracovníků objednatele);
    - vysvětlení všech použitých nastavení v rámci konfigurace a integrace do infrastruktury objednatele;
    - možné režimy uživatelského a administrativního přístupu a seznámení se základními i rozšířenými funkcemi;
    - způsob upgrade/update všech komponent;
    - nastavování pravidel;
    - vyhodnocování bezpečnostních incidentů;
    - vytváření reportů.

Veškeré činnosti zhotovitele musí být organizovány tak, aby nedošlo k výpadku žádného systému objednatele. Případné výpadky musí být naplánovány tak, aby neovlivnily provoz objednatele, tedy mimo běžnou pracovní dobu 7:00 – 18:00 v pracovních dnech.

Dokumentace musí zahrnovat alespoň:

- Technický popis prvků a jejich konfigurace. Dokumentace musí být zpracována v míře detailu, při které seznámená odborná osoba (úvodní

seznámení se správou a konfigurací dodaného systému) bude rozumět dané konfiguraci a důvodům její funkčnosti v daném prostředí.
- Informaci o znalostní bázi EDR řešení (může být vedena vendorem externě).
- Nouzový plán obnovy. Detailní plán obnovy v úrovni dostatečné pro osobu seznámenou se správou a konfigurací dodaného systému.
- Dokumentace bude obsahovat zejména technický popis, popis konfigurace, popis upgrade firmware, popis zálohy a obnovy konfigurace, schéma zapojení, a to v rozsahu potřebném pro konfiguraci a správu prostředí třetí osobou.
- Informace o způsobu updatovaní systému, agentů na koncových stanicích a řešení případných problémů s updatem.
- Diagramy skutečného provedení systému, návazností a vazeb v rámci jednotlivých částí.
- Instalační dokumentaci, popis změn vůči výchozím parametrům prostředí.

Záruční doba a technická podpora (nastavení parametrů SLA):

Záruční doba v délce trvání 36 měsíců od akceptace dodávky.

- objednatel má právo zakládat servisní tikety na helpdesku zhotovitele, případně i přímo u výrobce;
- součástí záruky je zajištění aktualizací SW i všech definic a databází po celou dobu záruky (produkt musí po celou dobu záruky plnit všechny požadavky z technické specifikace),
- reakce na řádně nahlášenou vadu max. do osmi (8) hodin od jejího nahlášení ve smluvených časech technické podpory a zahájení řešení do jednoho (1) pracovního dne po zadání incidentu.

Součástí služby technické podpory je podpora zhotovitele, konzultace, správa, vyhodnocování bezpečnostních incidentů, kontrola stavu systému a vyhodnocení logů v rozsahu minimálně 0,5 MD měsíčně, kterého se budou účastnit pracovníci objednatele;

Helpdesk:

Zhotovitel zajistí Helpdesk – jednotné kontaktní místo pro hlášení závad.

Vzdálený přístup:

Pro diagnostiku EDR řešení, resp. vzdálenou opravu, v případě problému bude zhotoviteli umožněno vzdálené připojení do sítě objednatele.

Příloha č. 2 – Seznam technických poradců

Seznam technických poradců, kteří jsou uvedeni v nabídce a splňují požadované technické kvalifikace Výzvy:

certifikace Trend Micro – Trend Vision One

rtifikace Trend Micro – Deep Security 20 Certified Proffesional

– certifikace Trend Micro – Trend Vision One XDR