KUPNÍ SMLOUVA

DNEŠNÍHO DNE, MĚSÍCE A ROKU:

Karlovarský kraj
se sídlem: Závodní 353/88, 360 06 Karlovy Vary
IČO: 70891168
DIČ: CZ70891168
bankovní spojení: UniCredit Bank 1387678928/2700
Raiffeisenbank 7882138002/5500
zastoupený: Ing. Jiřím Heliksem, vedoucím odboru informatiky Krajského úřadu Karlovarského kraje na základě usnesení Rady Karlovarského kraje č. RK 1065/09/22 ze dne 19. 9. 2022 a čl. VII odst. 1 písm. d) podpisového řádu

na straně jedné jako kupující (dále jen „kupující“)

a

Actinet Informační systémy s.r.o.
se sídlem: Olšanská 2643/1a, Žižkov, 130 00 Praha 3
IČO: 25552635
DIČ: CZ25552635
bankovní spojení: Raiffeisenbank a.s.
číslo účtu: 120777770/5500
zastoupený: Ing. Jiřím Račmanem, jednatelem společnosti
zapsaný v obchodním rejstříku vedeném Krajským soudem v Praze oddíl C vložka 67393

na straně druhé jako prodávající (dále jen „prodávající“)
(společně jako „smluvní strany“)

PREAMBULE

Vzhledem k tomu, že:

a) Prodávající je vybraným dodavatelem veřejné zakázky „**Zajištění bezpečnosti komunikačních sítí“** vyhlášené dne 24. 7. 2025 kupujícím jako zadavatelem veřejné zakázky malého rozsahu (dále jen veřejná zakázka); a

b) prodávající prohlašuje, že je držitelem potřebného živnostenského oprávnění a má řádné vybavení, zkušenosti a schopnosti, aby předmět koupě dle této smlouvy dodal ve stanovené době a ve sjednané kvalitě, a že si je vědom skutečnosti, že kupující má značný zájem na dodání předmětu koupě, který je předmětem této smlouvy, v čase a kvalitě stanovené touto smlouvou,

dohodly se smluvní strany na uzavření této

KUPNÍ SMLOUVY

(dále jen „smlouva“)

dle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

I. Předmět smlouvy

1.1 Prodávající se zavazuje za podmínek stanovených v této smlouvě odevzdat kupujícímu věc, která je předmětem koupě v množství, jakosti a provedení, jež je blíže specifikováno v nabídce prodávajícího podané dne 5. 8. 2025 (dále jen „nabídka“) v rámci zakázky **„Zajištění**

bezpečnosti komunikačních sítí“ a převést na něj vlastnické právo k předmětu koupě. Kupující se zavazuje předmět koupě převzít a zaplatit za něj prodávajícímu sjednanou kupní cenu.

1.2 Předmětem koupě je dodání softwarových licencí pro ochranu koncových zařízení na 3 roky včetně podpory výrobce a přístupu k aktualizacím, včetně implementace a 1 měsíc zvýšené podpory, zaškolení a poskytování technické podpory po dobu 3 let a je dále specifikován v příloze č. 1 smlouvy.

II. Dodání předmětu koupě

2.1 Prodávající je povinen odevzdat kupujícímu předmět koupě na sjednaném místě plnění, kterým je sídlo kupujícího.

2.2 Prodávající je povinen poskytnout (zprostředkovat poskytnutí) licence, které jsou součástí předmětu koupě nejpozději do **30. 10. 2025.** Technickou podporu bude prodávající poskytovat po dobu 3 let od uvedení do provozu.

2.3 Prodávající je povinen zajistit platnost licence po dobu 36 měsíců od implementace.

2.4 Prodávající se zavazuje po celou dobu platnosti licence poskytovat služby, které jsou součástí předmětu koupě.

III. Kupní cena

3.1 Kupní cena je cenou smluvní, nejvýše přípustnou, nepřekročitelnou a činí:

Cena bez DPH **1.095.000 Kč**

(slovy: jeden milion devadesát pět tisíc korun českých)

DPH **229.950 Kč**

(slovy: dvě stě dvacet devět tisíc devět set padesát korun českých)

Cena včetně DPH **1.324.950 Kč**

(slovy: jeden milion tři sta dvacet čtyři tisíc devět set padesát korun českých)

(dále jen „kupní cena“)

3.2 Kupní cena stanovená dle bodu 3.1 této smlouvy zahrnuje veškeré náklady prodávajícího spojené se splněním jeho závazku z této smlouvy, tj. cenu předmětu koupě včetně příslušenství a služeb, a dále zahrnuje zejména náklady na cestovné, licenční poplatky, úhradu cel a dalších nákladů spojených s celním řízením apod. Cena je stanovena jako nejvýše přípustná. Podrobná kalkulace celkové ceny předmětu koupě včetně jednotkových cen je uvedena v Příloze č. 2, která tvoří nedílnou součást této smlouvy.

3.3 Smluvní strany této smlouvy se dohodly, že prodávající, coby poskytovatel zdanitelného plnění, je povinen bez zbytečného prodlení písemně informovat kupujícího o tom, že se stal nespolehlivým plátcem ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty (dále jen „zákon o DPH“), ve znění pozdějších předpisů. Smluvní strany si dále společně ujednaly, že pokud kupující v průběhu platnosti tohoto smluvního vztahu na základě informace od prodávajícího či na základě vlastního šetření zjistí, že se prodávající stal nespolehlivým plátcem ve smyslu § 106a zákona o DPH, souhlasí obě smluvní strany s tím, že kupující uhradí za prodávajícího daň z přidané hodnoty z takového zdanitelného plnění dobrovolně správci daně dle § 109a zákona o DPH. Zaplacení částky ve výši daně kupujícím správci daně pak bude smluvními stranami považováno za splnění závazku uhradit sjednanou cenu, resp. její část. Smluvní strany si v této souvislosti poskytnou veškerou nezbytnou součinnost při vzájemném poskytování informací požadovaných zákonem o DPH. Prodávající současně souhlasí s tím, že je povinen kupujícímu nahradit veškerou škodu vzniklou v důsledku aplikace institutu ručení ze strany správce daně. Smluvní strany se dohodly, že kupující bude hradit sjednanou cenu pouze na účet zaregistrovaný a zveřejněný ve smyslu § 96 odst. 1 zákona o DPH.

IV. Platební podmínky a fakturace

4.1 Kupující nebude za dodání předmětu koupě poskytovat jakákoli plnění před dodáním předmětu koupě.

4.2 Kupní cena bude uhrazena po poskytnutí licencí na základě vystavené faktury. Splatnost faktury je smluvními stranami dohodnuta na 30 (třicet) kalendářních dnů ode dne řádného doručení faktury kupujícímu.

4.3 Faktura bude obsahovat náležitosti daňového dokladu stanovené zákonem o DPH a zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. V případě, že faktura nebude obsahovat správné údaje či bude neúplná, je kupující oprávněn fakturu vrátit ve lhůtě do data její splatnosti prodávajícímu. Prodávající je povinen takovou fakturu opravit, aby splňovala podmínky stanovené v tomto odstavci tohoto článku smlouvy. Lhůta splatnosti běží u opravené faktury od začátku. Objednatel je povinen přijmout elektronickou fakturu, v takovém případě upřednostňuje elektronickou fakturu ve formátu ISDOC zaslanou na epodatelna@kr-karlovarsky.cz, případně do datové schránky siqbxt2.

V. Smluvní pokuta

5.1 Smluvní strany se dohodly, že v případě porušení ustanovení čl. II. odst. 2.2 nebo 2.3 smlouvy prodávajícím, je kupující oprávněn uplatnit vůči prodávajícímu smluvní pokutu ve výši 0,05 % z kupní ceny včetně DPH, a to za každý i započatý den prodlení.

5.2 Smluvní strany se dohodly, že v případě porušení ustanovení čl. II. odst. 2.4 smlouvy prodávajícím, je kupující oprávněn uplatnit vůči prodávajícímu smluvní pokutu ve výši 5.000,- Kč za každou neposkytnutou službu, a to i opakovaně.

5.3 Smluvní strany se dohodly, že v případě, kdy kupující neuhradí bez zjevného důvodu kupní cenu do data splatnosti, může prodávající uplatnit vůči kupujícímu smluvní pokutu ve výši 0,05 % z dlužné částky, a to za každý i započatý den prodlení.

5.4 Smluvní pokuta je splatná do třiceti dní od data, kdy byla povinné straně doručena písemná výzva k jejímu zaplacení oprávněnou stranou, a to na účet oprávněné strany uvedený v písemné výzvě.

5.5 Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši.

VI. Odstoupení od smlouvy

6.1 Smluvní strany se dohodly, že mohou od této smlouvy odstoupit v případech, kdy to stanoví zákon, jinak v případě podstatného porušení této smlouvy. Odstoupení od smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé smluvní straně. Odstoupením od smlouvy se tato smlouva ruší od okamžiku doručení projevu vůle směřujícího k odstoupení od smlouvy druhé smluvní straně.

6.2 Smluvní strany se dohodly, že podstatným porušením smlouvy se rozumí zejména: jestliže se prodávající dostane do prodlení s dodáním předmětu koupě, ať již jako celku či jeho jednotlivých částí, ve vztahu k termínu dodání předmětu koupě dle této smlouvy, které bude delší než sedm kalendářních dnů.

6.3 V případě odstoupení od smlouvy ze strany kupujícího vzniká kupujícímu vůči prodávajícímu nárok na úhradu prokázaných vícenákladů (tj. nákladů vynaložených kupujícím nad kupní cenu za dodání předmětu koupě) vynaložených na dodání předmětu koupě a na úhradu ztrát vzniklých prodloužením termínu dodání předmětu koupě. Nárok kupujícího účtovat prodávajícímu smluvní pokutu tím nezaniká.

VII. Záruka za jakost

7.1 Délka záruční doby je dohodou smluvních stran sjednána na 36 měsíců. Běh záruční doby začíná ode dne odevzdání předmětu koupě kupujícímu.

7.2 Prodávajícím bude kupujícímu poskytován bezplatný záruční servis na kupujícím reklamované vady vzniklé v době trvání záruční doby.

7.3 Kupující je oprávněn reklamovat v záruční době vady předmětu koupě u prodávajícího, a to písemnou formou. V reklamaci musí být popsána vada, určen nárok kupujícího z vady, případně požadavek na způsob odstranění vad, a to včetně případného termínu pro odstranění vad prodávajícím. Kupující má právo volby způsobu odstranění důsledku vadného plnění.

7.4 Práva a povinnosti z prodávajícím poskytnuté záruky nezanikají ani odstoupením kterékoli ze smluvních stran od smlouvy.

7.5 O reklamačním řízení budou kupujícím pořizovány písemné zápisy ve dvojím vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran.

VIII. Doručování

8.1 Smluvní strany této smlouvy se dohodly následujícím způsobem na adrese pro doručování písemné korespondence:

a) adresa pro doručování kupujícímu je: Karlovarský kraj, Závodní 353/88, 360 06 Karlovy Vary.

b) adresa pro doručování prodávajícímu je: Olšanská 2643/1a, Žižkov, 130 00 Praha 3.

8.2 Veškerá podání a jiná oznámení, která se doručují smluvním stranám, je třeba doručit osobně, nebo doporučenou listovní zásilkou s doručenkou, pokud není ve smlouvě stanoveno jinak.

8.3 Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že oznámení bylo řádně doručené:

a) při doručování osobně:

- dnem faktického přijetí oznámení příjemcem; nebo
- dnem, v němž bylo doručeno osobě na příjemcově adrese určené k přebírání listovních zásilek; nebo
- dnem, kdy bylo doručováno osobě na příjemcově adrese určené k přebírání listovních zásilek, a tato osoba odmítla listovní zásilku převzít; nebo
- dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování dle článku 10., odst. 10.1 písm. a), b) této smlouvy.

b) při doručování prostřednictvím držitele poštovní licence:

- dnem předání listovní zásilky příjemci; nebo
- dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování dle článku 10., odst. 10.1 písm. a), b) této smlouvy.

c) při doručování do datové schránky:

- dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

IX. Závěrečná ustanovení

9.1 Prodávající bere na vědomí, že kupující je povinen uveřejnit tuto smlouvu ve smyslu 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.

9.2 Zaslání smlouvy do registru smluv zajistí kupující neprodleně po podpisu smlouvy. Kupující se současně zavazuje informovat prodávajícího o provedení registrace tak, že zašle prodávajícímu kopii potvrzení správce registru smluv o uveřejnění smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. již v průvodním formuláři vyplní příslušnou kolonku s ID datové schránky prodávajícího (v takovém případě potvrzení od správce registru smluv o provedení registrace smlouvy obdrží obě smluvní strany zároveň).

9.3 Smluvní strany této smlouvy se dohodly, že právní vztahy založené touto smlouvou se budou řídit právním řádem České republiky. Tato smlouva jakož i právní vztahy touto smlouvou neupravené se řídí úpravou zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

9.4 Případné spory vzniklé z této smlouvy budou řešeny dohodou smluvních stran a nebude-li dohody, pak podle platné právní úpravy věcně a místně příslušnými soudy České republiky.

9.5 V případě neplatnosti nebo neúčinnosti některého ustanovení této smlouvy nebudou dotčena ostatní ustanovení této smlouvy.

9.6 Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

9.7 Prodávající je povinen spolupůsobit při výkonu finanční kontroly ve smyslu § 2 písm. e) a § 13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonu (dále jen „zákon o finanční kontrole“), ve znění pozdějších předpisů, tj. poskytnout kontrolnímu orgánu doklady o dodávkách zboží a služeb hrazených z veřejných výdajů nebo z veřejné finanční podpory v rozsahu nezbytném pro ověření příslušné operace. Tutéž povinnost bude prodávající povinen požadovat po svých dodavatelích.

9.8 Tuto smlouvu lze měnit, doplňovat a upřesňovat pouze oboustranně odsouhlasenými, písemnými a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou smluvních stran, které musí být obsaženy na jedné listině.

9.9 Smlouva je vyhotovena ve třech stejnopisech, z nichž kupující obdrží dva výtisky a prodávající jeden výtisk. Každý stejnopis této smlouvy má právní sílu originálu.

Alternativně (před podpisem smlouvy se ponechá relevantní alternativa):

Tato smlouva je uzavřena elektronicky.

9.10 Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem uveřejnění v registru smluv.

9.11 Nedílnou součástí smlouvy jsou tyto přílohy:

Příloha č. 1: Vymezení předmětu plnění

Příloha č. 2: Cenová nabídka

9.12 Obě smluvní strany potvrzují autentičnost této smlouvy a prohlašují, že si smlouvu včetně příloh přečetly, s jejím obsahem (včetně příloh) souhlasí, že smlouva byla sepsána na základě pravdivých údajů, z jejich pravé a svobodné vůle a nebyla uzavřena v tísni ani za jinak jednostranně nevýhodných podmínek, což stvrzují svým podpisem, resp. podpisem svého oprávněného zástupce.

V ……dne ……..

Jiří Račman, Ing.
Digitally signed by Jiří Račman, Ing.
Date: 2025.09.05 10:25:05 +02'00'

prodávající

V Karlových Varech dne ……..

Ing. Jiří Heliks
P80060
Karlovarský kraj
Dne: 09.09.2025 07:58

kupující
Karlovarský kraj

Vymezení předmětu plnění

1. Předmět plnění

Předmětem plnění veřejné zakázky je zajištění bezpečnosti komunikačních sítí dle § 18 písm. a) – e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

2. Popis současného stavu

2.1. Popis lokalit

Serverovny jsou rozmístěny ve dvou budovách v areálu Krajského úřadu Karlovarského kraje. V těchto lokalitách bude probíhat poskytování poptávaných služeb.

2.2. Popis stávajícího HW prostředí

- TCKK je technicky i provozně navrženo, vybudováno a provozováno pro poskytování vysoce dostupných infrastrukturních ICT služeb Krajskému úřadu a jeho zřizovaným organizacím. Technologické centrum je napojeno na RKI – WAN na bázi optických vláken propojující významné úřady v kraji (vesměs obce s rozšířenou působností) a některé zřizované organizace kraje. Přenosová kapacity RKI páteřních spojů je 10 Gb/s.
- TCKK je tvořeno dvěma rovnocennými datovými centry, pouze zálohovací technologie jsou soustředěny pouze v jedné lokalitě.
- Serverová infrastruktura je tvořena dvěma Blade šasi HP c7000 osazených Blade servery Gen7 – Gen10. Šasi jsou vybavena redundantními 8Gb FC SAN přepínači, redundantními 1 GbE passtrought moduly a redundantními Virtual Connect Flex 10Gb moduly. 8 fyzických serverů je virtualizováno technologiemi VMware vSphere 7 Enterprise+. Všechny servery využívají k ukládání dat replikované datové úložiště Dell Unity.
- Datové úložiště se skládá z 2x Dell Unity 300 rozmístěné rovnoměrně do obou lokalit. Disková pole jsou doplněna odpovídající SAN FC 8 Gb infrastrukturou sestavenou z FC přepínačů Brocade. Délka optických tras mezi lokalitami je cca 300 metrů. Celková disková kapacita činí: 200 TB.
- V budově A Krajského úřadu je umístěn řídící a úložný server HP DL380 G8 zálohovacího systému Veeam Backup a Recovery Enterprise. Pro dlouhodobé ukládání záloh slouží pásková knihovna HPE MSL3040.
- Síťová vrstva je postavena na technologii Extreme Fabric Connect. V TCK je použita čtveřice přepínačů Extreme VSP 7400 a dvojicí Extreme 5420M propojené 100/25 GE linky a mezi Datacentry 40GE linky. Páteřní přepínače jsou dvojice přepínačů Extreme VSP 7400. Nacházejí se v rozvodných místnostech v budově A, B a jsou propojeny přes 40GE linky. Páteřní přepínače mají propojení do přepínačů Datacenter rovněž přes 40 GE a dále agregují linky z přístupových přepínačů z rozvodných míst jednotlivých budov areálu na rychlosti 10 Gbit/s. TCK je do RKI připojeno prostřednictvím redundantních centrálních prvků HPE 5900-AF.
- Inspekci a řízení internetového provozu zajišťuje perimetrový firewall Checkpoint, který slouží i pro publikaci některých služeb TCKK bez pokročilých ochran a autentizačních mechanismů.
- Publikace většiny služeb TCKK do Internetu a RKI je prováděno prostřednictvím F5 Big-IP.
- Distribuční a přístupová vrstva síťové infrastruktury využívá síťové prvky Extreme na technologii Extreme Fabric Connect. Pro bezdrátovou komunikaci jsou využívány prvky Extreme.
- Obě lokality jsou vybaveny motorgenerátory, překlenutí doby jejich náběhu a krátkodobých výpadků zajišťují UPS EATON 9355.
- Datová centra jsou dále vybavena klimatizacemi, zhášecím systémem, IP kamerami a Rack management systémem (dále RMS) s kouřovými, pohybovým a vlhkostními čidly s možností zasílání varování přes SMS.

2.3. Popis stávajícího SW prostředí

- Systémové služby jsou provozovány převážně na platformě Microsoft, jde zejména o následující systémy:
  - Microsoft Windows Server Datacenter a Standard
  - Microsoft SQL Standard
  - Microsoft Exchange Standard
  - Microsoft 365
- Verze systémů Microsoft jsou průběžně aktualizovány v konzervativním režimu, tj. jsou udržovány cca. 1-2 verze za aktuální verzí.
- Pro doručování aplikací uživatelům jsou využívány technologie Microsoft Remote Desktop Service
- Primární adresářovou službou je Active Directory provozovaná na redundantních replikovaných řadičích, které zajištují také služby DNS a DHCP.
- K ukládání sdílených souborů je kromě prostředků Windows serveru využívána NAS funkcionalita diskového pole Dell Unity.
- Virtualizační platformou TCKK je VMware vSphere 7 Enterprise+ řízená jedním vCentrem. Jsou implementovány a využívány pokročilé funkce vSphere – High availability, Dynamic Resource Scheduler, vMotion, virtuální switche apod.

2.4. Popis způsobu řešení incidentů

- Zadavatel pro řešení incidentů a podporu uživatelů používá interní HelpDesk vytvořený na zakázku.
- Incidenty a požadavky uživatelů se řeší formou ticketů v systému HelpDesk, uživatelé tak mají přehled o stavu řešení jejich požadavků. Zadavatel také zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.
- Incidenty a požadavky, které nevyřeší interní HelpDesk budou předávány do helpdeskového systému dodavatele provozní podpory. Hlášení incidentů a požadavků bude prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

2.5. Popis servisních oken

TCKK nemá pevně definovaná pravidelná servisní okna. Aplikace aktualizací a oprav virtuálních serverů provádějí zaměstnanci KÚKK dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.

3. Požadavky na technické řešení

3.1. Základní požadavky

Cílem projektu zajištění bezpečnosti komunikačních sítí dle § 18 písm. a) – e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Požadavky:

- nabízené řešení bude obsahovat SW komponenty jednoho výrobce včetně managementu,
- podpora dodávaného řešení bude dodavatelem zajištěna na období 3 let včetně aktualizací funkcionalit
- součástí 3leté technické podpory dodavatele bude:
  - odstranění náhlých závad na SW vybavení
  - pravidelná měsíční kontrola stavu systému
  - update systému (minor verze, patche) 2x ročně
  - dodavatel poskytne objednateli přístup do svého ticketovacího systému (ServiceDesk), ve kterém bude prováděno hlášení závad nebo požadavků a dodavatel je povinen vést k těmto požadavkům objednatele v systému evidenci
  - činnosti dodavatele v rámci technické podpory budou provozovány v režimu 5x8, tj. po dobu 5 pracovních dnů v týdnu v době mezi 8 a 16 h

    - dodavatel oznámí objednateli jméno řešitele požadavku nejpozději do 1 hodiny od jeho nahlášení v tiketovacím systému dodavatele
    - dodavatel zahájí činnosti spojené s odbavením požadavku zadavatele nejpozději následující pracovní den po nahlášení požadavku v ticketovacím systému (servicedesk) dodavatele
- nabízené řešení bude instalováno na tzv. koncová zařízení zadavatele,
- nabízené řešení bude spravováno z centrálního managementu,
- nabízené řešení, jehož součástí je EDR řešení musí obsahovat agenta minimálně do prohlížeče Chrome, Firefox, Brave, Edge,
- nabízené řešení musí být schopno současného provozování různých verzí agenta, tzn. dle požadavku zadavatele může být na určitém typu koncových zařízeních nainstalována jiná verze než na jiném typu koncových zařízeních,
- nabízené bezpečnostní řešení EDR bude provádět nepřetržitý sběr dat a analýzu s hlášením do centralizovaného systému. To poskytne bezpečnostnímu týmu plný přehled o stavu koncových bodů sítě,
- nabízené bezpečnostní řešení EDR bude provádět automatizovaný sběr a zpracování dat a určité činnosti odezvy. To umožní bezpečnostnímu týmu rychle získat kontext týkající se potenciálního bezpečnostního incidentu a rychle podniknout kroky k jeho nápravě,
- nabízené bezpečnostní řešení umožní automatické aktivní reakce na incidenty na základě předem definovaných pravidel. To umožní zablokovat nebo rychle reagovat na nežádoucí aktivity. Průběžný sběr a analýza dat řešení EDR poskytuje detailní přehled o stavu koncových stanic.

3.2. Centralizovaný nástroj pro správu

Požadované funkcionality:

- centrální správa dodaného SW, prostřednictvím centrálního management v Cloudu nebo On premise v DC zadavatele,
- přiřazení uživatelských oprávnění dle rolí,
- dlouhodobé uchování záznamů alespoň 90 dnů,
- rozhraní pro reporting – vytváření reportů o provozu z uchovaných záznamů.

3.3. Požadavky na funkcionality řešení

Požadované funkcionality:

Threat Intelligence:

Požadujeme prevenci hrozeb založenou na kombinaci informací o hrozbách ze sdílených databází (tzn. výrobce SW musí mít přístup k databázi sdílené s jinými poskytovateli) kombinovanou s pokročilými technologie umělé inteligence, aby byla navýšena oblast prevence. Požadujeme schopnost řešení přidávat Indikátory kompromitace IoC pro domény, IP adresy, URL, MD5 Hash klíče a SHA1 Hash klíče, které umožní řešení jejich automatickou blokaci.

Access Control:

Požadujeme spolupráci s naším řešení FW Check Point tak, aby pravidla brány firewall přijímaly nebo rušily síťový provoz do a z koncových bodů na základě IP adres, domén, portů a protokolů.

Požadujeme možnost omezit přístup k síti pro konkrétní aplikace tak, aby bylo možno definovat, zda povolit, blokovat nebo ukončit aplikace a procesy.

Požadujeme, aby řešení umožnilo zajistit pro koncové body dodržování bezpečnostních pravidel organizace. Koncové body, které pravidla nebudou splňovat se zobrazí jako „nesouladné“ a správce na ně může použít omezující zásady.

Threat Prevention:

Požadované řešení musí neustále monitorovat chování specifické pro ransomware a identifikovat nelegitimní šifrování souborů bez signatury. Musí detekovat a uplatňovat karanténu všech prvků útoku ransomwaru, které jsou identifikovány forenzní analýzou.

Požadujeme zajištění plné kontinuity provozu tak, aby šifrované soubory byly automaticky obnoveny ze snapshotů.

Požadujeme funkcionalitu Intel TDT – Implementace ochrany na úrovni procesoru pomocí technologie Intel Threat Defense.
Požadované řešení musí chránit před malwarem resp. před všemi druhy malwarových hrozeb, červů, trojských koní a adware.
Řešení musí být schopnou funkce Anti-Bot, kdy požadujeme zabránění dopadům infekce Bot na koncové body.
Požadujeme ochranu před útoky založenými na exploitech, které ohrožují legitimní aplikace, a požadované řešení zajistí, že tyto zranitelnosti nelze zneužít.
Požadujeme, aby řešení detekovalo a blokovalo mutace malwaru podle jejich chování v reálném čase.
Požadujeme ochranu portů tím, že řešení bude vyžadovat autorizaci pro přístup k úložným zařízením a dalším vstupně/výstupním zařízením.
Analytické funkce:
Požadujeme, aby se po detekci škodlivé události automaticky spustila forenzní analýza a celá sekvence útoku byla prezentována jako forenzní zpráva.
Požadujeme tzv. mapování MITRE, kdy řídicí panel MITRE ATT&CK poskytuje přehled o všech technikách pozorovaných aplikací pro ochranu koncového bodu v reálném čase a mapuje všechny události na MITRE taktiky, techniky a postupy (TTPs).
Ochrana prohlížeče:
Součástí řešení musí být agent do prohlížeče minimálně pro Chrome,Firefox, Brave, Edge a musí:

- detekovat phishingove webové stránky,
- umožňovat CDR (Content Disarm and Reconstruction) stahovaných souborů,
- detekce použití firemních přístupových údajů při přihlášení na 3rd party webové služby,
- vynutit "safe search",
- podporovat URL filtering,
- možnost rozšíření o podporu DLP funkcionality pro upload souborů,
- možnost rozšíření o DLP nad GenAI (ChatGPT a další GenAI produkty).

Zajistit Zero-Phishing ochranu v reálném čase před neznámými zero-day phishingovými stránkami. Statická a heuristická detekce podezřelých prvků na webových stránkách, které vyžadují soukromé informace.
Vynutit ochranu firemních přihlašovacích údajů tzn. detekovat opakované použití firemních přihlašovacích údajů na externích stránkách.
Umožnit filtrování URL díky plugin prohlížeče, který povoluje/blokuje přístup k webovým stránkám v reálném čase s plným přehledem o provozu HTTPS.
Zajistit bezpečné vyhledávání. Tzn. z našeho pohledu funkci přidanou do vyhledávačů, která funguje jako automatizovaný filtr pro potenciálně urážlivý a nevhodný obsah.
Možnost rozšíření o zabezpečení DLP a GenAI funkce, což zahrnuje možnost skenování nahrávání a stahování, ovládání schránky a tisku a bezpečnostní nástroje GenAI pro detekci a prevenci ztráty dat v reálném čase. To vše s více než 700 předdefinovanými datovými typy a Microsoft Tagging option.
Posture Management:
Požadujeme funkce tzv. Posture Managementu, které obsahují Vulnerability Management and Patch Management, kdy tyto funkcionality poskytují automatickou detekci zranitelností, stanovují priority a opravy, pro snížení rizika narušení dat nebo jiného bezpečnostního incidentu.

3.4. Obecné požadavky

Na veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:

- mají plnou záruku od výrobce,
- mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
- obsahují všechny nezbytné licence na používání příslušného softwaru,
- jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
- jsou určeny pro provoz v České republice.

- Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.
- Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.
- Navržené řešení musí být tvořeno komponentami podle uvedených požadavků.
- Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
- Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.
- Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
- Veškeré dodávané HW a SW produkty musí být získány legálně a umožňovat využití těchto produktů zadavatelem, jako koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce.
- V případě dodání HW a SW produktů zadavateli, jako koncovému zákazníkovi, nesmí být zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje. Uvedené musí zahrnovat i nárok zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání podpory výrobce.
- Musí být umožněn online přístup Zadavatele k dokumentaci výrobce HW/SW a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží a licencí / subscripcí / operačních systémů.
- Dodavatel musí garantovat, že v případě dodání zboží Zadavateli, jako koncovému zákazníkovi, bude Dodavatelem poskytnuta k dodávanému zařízení záruka a produktová podpora v plném, poskytovaném rozsahu.
- Součástí všech zařízení musí být dodávka SW a firmware v aktuální verzi.
- Dodavatel může nabídnout řešení a zboží s lepšími parametry (v případě, že lze objektivně stanovit, že se jedná o parametry lepší), nikoliv s parametry horšími (či horší kvality), než požaduje zadavatel v zadávacích podmínkách. Zadavatel připouští i jiná kvalitativně a technicky obdobná řešení za podmínky, že nesmí dojít ke zhoršení požadovaných parametrů.

4. Implementace

Zadavatel požaduje implementaci výše uvedeného HW a SW a to v tomto rozsahu:

- Vypracování technicko-implementačního projektu s popisem budoucího stavu a plánem migrace na novou infrastrukturu i s akceptačními testy,
- Vypracování dokumentace skutečného provedení a provozní dokumentace.
- Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností specialisty maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
- Činnost omezující práci uživatelů musí být prováděny mimo běžnou pracovní dobu úřadu, tj. mimo pracovní dny 7 – 15 hod.

5. Požadavky na testovací prostředí.

- Zadavatel nedisponuje testovacím prostředím,

- Vyžaduje-li Uchazeč pro realizaci zakázky testovací prostředí, zahrne do nabídky náklady na jeho vybudování a požadovanou součinnost Zadavatele.

6. Obecné požadavky na provedení akceptačních testů a přechod do ostrého provozu

a) Uchazeč navrhne způsob a provedení akceptačních testů. Součástí akceptačních testů musí být pro každou komoditu minimálně:
   i. Prokázání kompletnosti dodávky a splnění povinných parametrů a požadavků,
   ii. Prokázání funkčnosti migrovaných systémů,
   iii. Prokázání aktivací aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

b) Pro každý systém či modul navrhne Uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost, bezpečnost a odpovídající výkon a stabilita dodaného řešení,

c) O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol,

d) Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

7. Součásti nabídky

- Nabídka musí obsahovat následující položky:
  - Cenu za 500 ks SW licencí pro ochranu koncových zařízení splňujících plně technické požadavky Zadavatele,
  - Cenu takového řešení na 3 roky včetně podpory výrobce a přístupu k aktualizacím,
  - Cenu za uvedení do provozu tzn. implementace a 1 měsíc zvýšené podpory,
  - Cenu za 3 roky poskytování ServiceDesku a Heldesku Dodavatele v režimu 9x5,
  - Cenu za zaškolení administrátorů:
    - distribuce licencí uživatelům
    - dohled
    - aktualizace SW
    - řešení obvyklých poruchových stavů
    - tvorba pravidel pro všechny typy bezpečnostních funkcionalit
  - Informaci o minimálních provozních požadavcích jak pro agenta, tak pro management

8. Technická kvalifikace

V rámci technické kvalifikace zadavatel požaduje předložit:

1) Seznam významných dodávek nabízené technologie poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny a doby jejich poskytnutí a identifikace objednatele.

   Stanovení minimální úrovně

   a) Zadavatel stanovuje, že za významnou dodávku se považuje:
      - Dodávka a implementace ochrany koncového bodu na nabízené technologii do prostředí objednatele a poskytování technické podpory a zároveň

   b) Zadavatel dále stanovuje, že v seznamu významných dodávek musí být uvedeny minimálně:
      - 2 významné dodávky podle předchozího bodu 1) a zároveň

   c) Zadavatel stanovuje minimální výši (hodnotu) významných dodávek následovně:
      - Každá významná dodávka dle předchozího bodu 1) musí dosahovat výše minimálně 1 milion Kč bez DPH.

2) Seznam techniků, kteří se budou podílet na plnění veřejné zakázky
   Stanovení minimální úrovně:
   a) Technici, kteří se budou podílet na plnění veřejné zakázky – realizační tým se musí skládat minimálně z těchto rolí:

      - 2x Technický specialista pro implementaci technologie pro ochranu koncových bodů
      - 1x Technický specialista pro implementaci firewallů z důvodu nastavení vzájemné komunikace obou řešení

   b) Specifikace minimálních požadavků na technického specialistu

Označení role	**Technický specialista pro implementaci technologie pro ochranu koncových bodů**
Profesní praxe v oblasti kyberbezpečnosti	Min. 5 let
Požadovaná certifikace	Platný technický certifikát výrobce nabízené technologie dokládající jeho způsobilost
Účast na zakázkách	Profesní zkušenost s realizací alespoň 3 projektů spočívajících v dodávce a implementaci technologie pro ochranu koncových bodů

Tabulka č.1 - Kvalifikace – Technický specialista pro implementaci technologie pro ochranu koncových bodů

Označení role	**Technický specialista pro implementaci firewallů**
Profesní praxe v oblasti implementace síťových technologií	Min. 5 let
Požadovaná certifikace	Platný technický certifikát výrobce nabízené technologie dokládající jeho způsobilost
Účast na zakázkách	Profesní zkušenost s realizací alespoň 2 projektů spočívajících v dodávce a implementaci Firewallů

Tabulka č.2 - Kvalifikace – Technický specialista pro implementaci firewallů

Výše uvedené požadavky uchazeč prokáže v nabídce prostřednictvím předložení strukturovaného profesního životopisu každého jednotlivého člena realizačního týmu a předložením kopií odborných technických certifikátů rovněž každého jednotlivého člena realizačního týmu.

Uchazeč ve své nabídce rovněž předloží certifikát nebo potvrzení výrobce nabízené technologie o obchodním partnerství

Odborné a technické certifikáty, jakož i certifikáty o obchodním partnerství budou akceptovány v českém, slovenském nebo anglickém jazyku.