

Smlouva o dodávce, implementaci a technické podpoře řešení pro zvýšení kybernetické bezpečnosti informačních a komunikačních systémů

(dále jen „**Smlouva**“)

uzavřená ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), za přiměřeného použití § 2358 a násl. občanského zákoníku, § 2586 a násl. ve spojení a § 2631 a násl. občanského zákoníku, a dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským (dále jen „autorský zákon“)

mezi těmito smluvními stranami:

Objednatel:	Město Holešov
se sídlem:	Masarykova 628, 769 01 Holešov
zastoupen:	Mgr. Milanem Fritzem, starostou
IČO:	00287172
Bankovní spojení:	Komerční banka, a.s.
Číslo účtu:	██████████

(dále také jako „**Objednatel**“ či „**Nabyvatel**“)

Dodavatel:	Aricoma Systems a.s.
se sídlem:	Hornopolská 3322/34, Moravská Ostrava, 702 00 Ostrava
zastoupen:	Jaroslavem Dvořákem, členem představenstva Tomášem Ječmínkem, členem představenstva
Zapsán OR:	sp. zn. B 11012 vedená u Krajského soudu v Ostravě
kontaktní osoba ve věcech smluvních:	Jaroslav Dvořák, člen představenstva Tomáš Ječmínek, člen představenstva
kontaktní osoba ve věcech technických:	██████████
IČO:	043 08 697
DIČ:	CZ04308697
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	██████████

(dále také jako „**Dodavatel**“ či „**Poskytovatel**“)

(společně jako „**smluvní strany**“ či jednotlivě jako „**smluvní strana**“)

uzavřely tuto Smlouvu na základě výsledku zadávacího řízení na veřejnou zakázku s názvem „Zajištění kybernetické bezpečnosti na MěÚ Holešov“.

I. ÚVODNÍ USTANOVENÍ

1. Objednatel zahájil veřejnou zakázku s názvem „Zajištění kybernetické bezpečnosti na MěÚ Holešov“, přičemž nabídka Dodavatele byla vybrána jako nejvhodnější.
2. Na základě této Smlouvy má Dodavatel ve prospěch Objednatele dodat řešení pro zvýšení kybernetické bezpečnosti Objednatele, provést jeho implementaci do infrastruktury Objednatele, a zajistit technickou podporu tohoto řešení, a to za podmínek dále uvedených v této Smlouvě a jejích přílohách.
3. Závazek mezi smluvními stranami založený touto Smlouvou se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „autorský zákon“).
4. Tato Smlouva je uzavřena na základě výsledku zadávacího řízení vedeného podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“). Jednotlivá ustanovení této Smlouvy musí být vykládána v souladu se zadávacími podmínkami uvedenými v zadávací dokumentaci veřejné zakázky, vč. jejich příloh, a v souladu s nabídkou Dodavatele podanou v rámci zadávacího řízení veřejné zakázky.
5. Účelem uzavření Smlouvy je dodávka komponent softwarové (SW) a hardwarové (HW) infrastruktury a jejich instalace, implementace a vzájemná integrace na stávající informační systémy Objednatele za účelem zvýšení kybernetické bezpečnosti Objednatele, a posílení schopnosti odolávat vnějším kybernetickým hrozbám.
6. Na realizaci projektu byla přislíbena finanční podpora Národního plánu obnovy. Dodavatel je povinen poskytnout objednateli veškerou součinnost tak, aby financování projektu nebylo ohroženo. Dodavatel je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do konce roku 2036.

II. PROHLÁŠENÍ SMLUVNÍCH STRAN

1. Dodavatel prohlašuje, že je plně způsobilý k řádnému a včasnému provedení předmětu této Smlouvy, že se řádně seznámil s rozsahem a povahou předmětu Smlouvy, a to takovým způsobem, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k jeho realizaci, a že disponuje takovými kapacitami a odbornými znalostmi, vlastním technickým vybavením a zázemím, které jsou nezbytné pro realizaci předmětu Smlouvy za dohodnuté smluvní ceny uvedené v této Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.
2. Dodavatel je oprávněn plnit předmět této Smlouvy pouze prostřednictvím svých zaměstnanců nebo osob uvedených v seznamu poddodavatelů (příloha č. 3 této Smlouvy).
3. Dodavatel dále prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Rovněž prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Dodavatele a že takové exekuční řízení nebylo vůči němu zahájeno.

4. Smluvní strany prohlašují, že identifikační údaje smluvních stran uvedené v této Smlouvě odpovídají aktuálnímu stavu, a že osobami jednajícími při uzavření této Smlouvy jsou osoby oprávněné k jednání za smluvní strany. Jakékoliv změny předmětných údajů, jež nastanou v době po uzavření této Smlouvy, jsou smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé smluvní straně.
5. V případě, že se kterékoliv prohlášení některé ze smluvních stran podle tohoto článku Smlouvy ukáže být nepravdivým, odpovídá tato smluvní strana za škodu a nemajetkovou újmu, která nepravdivostí prohlášení nebo v souvislosti s ní druhé smluvní straně vznikne.
6. Dodavatel a Objednatel se zavazují k vzájemné součinnosti za účelem plnění předmětu této Smlouvy.

III. PŘEDMĚT SMLOUVY

1. Předmětem této Smlouvy je závazek Dodavatele dodat komponenty softwarové (SW) a hardwarové (HW) infrastruktury, provést jejich instalaci, implementaci a vzájemnou integraci, zejména provést:
 - 1.1. zabezpečení komunikační sítě a segmentace sítě (pořízení switchů pro zajištění segmentace sítě a řízení přístupu ke službám sítě),
 - 1.2. pořízení a implementace nástroje pro multifaktorovou autentizaci (dodávka aplikace pro řízení přístupu k službám a datům informačních systémů pomocí druhého faktoru),
 - 1.3. pořízení a implementace nástroje pro ochranu a zabezpečení e-mailů,
 - 1.4. pořízení a implementace nástroje z kategorie Advanced Threat Protection (Ochrana koncových stanic před internetovými útoky (ATP) přinese sjednocenou platformu pro preventivní ochranu, detekci porušení zabezpečení, automatizované prověřování a reakci na útoky),
 - 1.5. pořízení a implementace nástroje pro analýzu a monitoring síťového provozu (Systém pro správu bezpečnostních událostí, který obsahuje detekční prvky pro neobvyklé a potenciálně škodlivé události včetně schopnosti automatické reakce na incident),
 - 1.6. pořízení a implementace nástroje pro log management (nástroj pro systematizovaný sběr logů napříč infrastrukturou s funkcemi usnadňujícími seskupování logů podle věcné a časové souvislosti umožňující technickému správci dohledávat příčiny kybernetických incidentů),
 - 1.7. pořízení a implementace nástroje pro ochranu počítačové sítě před malwarem a zneužíváním zařízení na úrovni DNS překladu, řešení poskytujícího plnou kontrolu nad DNS provozem,
 - 1.8. pořízení serverů, softwarově definovaných úložišť, potřebných licencí a zálohovacích NAS (budou přímo využita v rámci zajištění kybernetické bezpečnosti – virtualizace, ukládání logů, zajištění vysoké úrovně dostupnosti informací, aj.)
 - 1.9. poskytnout Objednateli veškeré potřebné licence k dodanému řešení,
 - 1.10. provést zaškolení administrátorů a uživatelů na straně Objednatele,
 - 1.11. provést zkušební provoz a akceptační testy,
 - 1.12. zpracovat a předat Objednateli veškerou dokumentaci dodaného a implementovaného řešení do infrastruktury Objednatele,

- 1.13. zajistit projektové vedení po celou dobu realizace plnění,
- 1.14. poskytnout standardní záruku na dodané řešení,
- (dále společně jako „**předmět plnění**“).
2. Předmětem této Smlouvy je rovněž závazek Dodavatele:
- 2.1. poskytnout Objednateli **nadstandardní (prodlouženou) záruku**,
- 2.2. poskytnout Objednateli **technickou podporu (maintenance support + základní technická podpora)** dodaného a implementovaného řešení po dobu udržitelnosti projektu (min. 60 měsíců od jeho předání Objednateli).
3. Minimální technické, funkční a implementační/integrační požadavky na předmět plnění, a požadavky na poskytování dalších služeb, jak jsou vymezeny Objednatelem, a v rozsahu, v jakém se je zavázal naplňovat Dodavatel pro celou dobu plnění této Smlouvy, jsou závazně uvedeny v příloze č. 1 této Smlouvy.
4. Dodavatelem nabízený předmět plnění a zejména způsob jeho provedení musí splňovat požadavky stanovené vyhláškou 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).
5. Dodavatel poskytne Objednateli předmět plnění na základě písemného projektu, který bude obsahovat zejména:
- 5.1. popis dodávaného řešení (specifikaci dodávaného HW a SW, funkční schéma řešení),
- 5.2. popis způsobu a postupu implementace do infrastruktury Objednatele,
- 5.3. popis zabezpečení dodávaného řešení včetně zabezpečení informačních a komunikačních systémů v průběhu provádění díla,
- 5.4. popis plánu zálohování a obnovy síťové infrastruktury,
- 5.5. plán zkušebního provozu a provedení akceptačních testů,
- 5.6. plán zaškolení administrátorů a uživatelů,
- 5.7. harmonogram postupu prací v členění minimálně na kalendářní týdny,
- 5.8. požadavky na součinnost Objednatele a období pro poskytnutí takové součinnosti, aj.
- (dále jen „**prováděcí projekt**“).
6. Dodavatel prohlašuje, že je oprávněn k distribuci programů a služeb, jež tvoří předmět této Smlouvy vymezený v předchozím odst. 1. tohoto článku Smlouvy, a touto Smlouvou poskytuje Objednateli oprávnění k jeho využívání v rozsahu a za podmínek v této Smlouvě vymezených.
7. Dodavatel se zavazuje, že využije ke zhotovení předmětu plnění pro Objednatele takové hardwarové či softwarové produkty a technologie, o kterých na základě své odbornosti a dostupných roadmap výrobců ví či může předpokládat, že budou schopny plnit účel vyplývající z této Smlouvy a budou výrobcem podporovány nejméně po dobu 60 měsíců od okamžiku dokončení předmětu plnění dle předpokladů stanovených touto Smlouvou a jejími přílohami. Tato skutečnost bude posuzována k datu podání nabídky Dodavatele, která předcházela uzavření této Smlouvy. Dodavatel splní tento závazek zejména tehdy,

využije-li takové hardwarové či softwarové produkty a technologie, o nichž bylo v době podání nabídky před uzavřením této Smlouvy známo, že pro ně není vyhlášeno datum ukončení prodeje (end of sale), ani datum ukončení podpory/servisu (end of support/service). Nesplnění podmínky dle předchozí věty se považuje za vadu plnění, pro kterou je Objednatel oprávněn plnění Dodavatele nepřevzít, a to až do okamžiku odstranění takové vady, zjistí-li tak před převzetím plnění; v ostatních případech bude Objednatel postupovat podle čl. XIII. odst. 3. této Smlouvy. Porušení uvedeného závazku a nezjednání nápravy dle této Smlouvy se považuje za podstatné porušení Smlouvy.

8. Předmětem této Smlouvy je závazek Objednatele zaplatit za Dodavatelem poskytnutý předmět plnění cenu sjednanou v čl. VI. této Smlouvy, v rozsahu Dodavatelem poskytnutého předmětu plnění dle přílohy č. 1 této Smlouvy a dle položkového ocenění podle přílohy č. 2 této Smlouvy.

IV. MÍSTO A DOBA PLNĚNÍ

1. Místem plnění je adresa sídla Objednatele: Masarykova 628, 769 01 Holešov. Smluvní strany předpokládají poskytování předmětu plnění rovněž prostřednictvím dálkové komunikace a vzdáleného přístupu.
2. Dodavatel se zavazuje zahájit provádění předmětu plnění bezodkladně po nabytí účinnosti této smlouvy.
3. Smluvní strany se dohodly, že provádění předmětu plnění a jeho harmonogram bude respektovat jako nejzazší níže uvedené uzlové body (milníky):

Označení milníku	Název milníku	Trvání (nejpozději do)
T0	Zahájení plnění	po nabytí účinnosti Smlouvy
T1	Předložení prováděcího projektu Objednateli k akceptaci (akceptační protokol/prohlášení)	T0 + 4 kalendářní týdny
T2	Dodávka a implementace řešení – kyberbezpečnostní opatření (akceptační protokol/prohlášení)	T0 + 24 kalendářních týdnů
T3	Zpracování a předání dokumentace dodaného a implementovaného řešení; Školení administrátorů (akceptační protokol/prohlášení)	T0 + 26 kalendářních týdnů
T4	Zkušební provoz a akceptační testy (akceptační protokol/prohlášení)	T0 + 28 kalendářních týdnů
T5	Předání a převzetí dokončeného řešení a zahájení ostrého provozu (protokol o předání a převzetí předmětu plnění)	T0 + 28 kalendářních týdnů
T6	Poskytování technické podpory	T5 + 60 měsíců

4. Smluvní strany se dohodly, že podmínkou pro zahájení dodávky a implementace řešení do infrastruktury Objednatele (T2) je písemná akceptace prováděcího projektu Objednatelem. Objednatel se zavazuje provést posouzení prováděcího projektu dle čl. III. odst. 5. této Smlouvy a sdělit výsledek tohoto posouzení bez zbytečného odkladu po jeho předložení Dodavatelem, nejpozději však do 3 pracovních dnů od jeho předložení Dodavatelem. Za účelem dosažení akceptace prováděcího projektu Objednatelem ve lhůtě dle milníku T1 je Dodavatel oprávněn průběžně seznamovat Objednatele se stavem a obsahem

tohoto prováděcího projektu. Objednatel je oprávněn vyzvat Dodavatele k poskytnutí rozpracované verze prováděcího projektu.

V případě, že prováděcí projekt nebude Dodavatelem zpracován v souladu s čl. III. odst. 5. této Smlouvy a/nebo bude vykazovat takové vady či nedostatky, v jejichž důsledku by bylo ohroženo naplnění účelu této Smlouvy vyjádřeného v čl. I. odst. 5. této Smlouvy, je Objednatel oprávněn odepřít akceptaci prováděcího projektu a sdělit důvody takového odepření akceptace. Nedojde-li k odstranění důvodů vedoucích k odepření akceptace prováděcího projektu ani v dodatečně lhůtě stanovené dohodou smluvních stran, je Objednatel oprávněn od této Smlouvy odstoupit. V případě akceptace prováděcího projektu Objednatelem v dodatečně lhůtě stanovené dohodou smluvních stran není dotčena odpovědnost Dodavatele za případné prodloužení se splněním milníků dle předchozího odst. 3. tohoto článku Smlouvy. Odstoupí-li Objednatel od Smlouvy z důvodu uvedeného v tomto odstavci Smlouvy, nevzniká Dodavateli jakýkoliv nárok na úhradu ceny plnění či její části.

5. Smluvní strany se dohodly, že řádná a včasná dodávka a implementace řešení do infrastruktury Objednatele, včetně úspěšného absolvování zkušebního provozu, bude Dodavatelem předána Objednateli tak, aby Objednatel akceptoval a převzal dokončené řešení nejpozději **do 28 kalendářních týdnů ode dne nabytí účinnosti této Smlouvy**.
6. Smluvní strany se dohodly, že technická podpora bude Dodavatelem poskytována po dobu 60 měsíců ode dne akceptace a převzetí dokončeného řešení Objednatelem, není-li dále v této Smlouvě uvedeno jinak. Po uvedené období bude zajištěna platnost a trvání veškerých poskytnutých licencí.

V. PŘEDÁNÍ (ČÁSTI) PŘEDMĚTU PLNĚNÍ, AKCEPTACE

1. Smluvní strany se dohodly na tom, že Objednatel není povinen předmět plnění či jeho část převzít (akceptovat), pokud vykazuje vady či nedodělky, nenaplní veškeré požadavky, k jejichž splnění se Dodavatel zavázal, zejména pak požadavky plynoucí z přílohy č. 1 této Smlouvy anebo z prováděcího projektu, který Dodavatel předložil; zejména pak Objednateli náleží právo nepřevzít (neakceptovat) předmět plnění nebo jeho dílčí část v případě, kdy taková vada, nedodělek či rozpor s výše uvedenými dokumenty brání řádnému užívání předmětu plnění, resp. při návaznosti jednotlivých milníků dle čl. IV. odst. 3. této Smlouvy brání taková vada, nedodělek či rozpor v zahájení navazujícího milníku. Zároveň Objednatel není povinen předmět plnění převzít, pokud není proveden včas.
2. Akceptací předmětu plnění Objednatelem se závazek Dodavatele považuje za splněný, a výsledek plnění Dodavatele za způsobilý k užívání Objednatelem.
3. Akceptací předmětu plnění Objednatelem bude předcházet ověření, zda plnění poskytnuté Dodavatelem dle této Smlouvy vedlo k výsledku a naplnění účelu, ke kterému se smluvní strany zavázaly, a to porovnáním skutečných vlastností jednotlivých částí plnění poskytnutých Dodavatelem dle této Smlouvy s jednotlivými požadavky pro ně stanovenými v této Smlouvě.
4. Předmět plnění se považuje za akceptovaný okamžikem podpisu příslušného protokolu ze strany Objednatele. Formálními náležitostmi protokolu o předání a převzetí předmětu plnění je jeho označení, datum vystavení, celkový počet stran, označení Smlouvy, označení Dodavatele a Objednatele, název projektu, označení a popis plnění, které je předmětem akceptace, datum zahájení a ukončení plnění, jméno a podpis osob, které protokol podepsaly. Protokol bude vyhotoven ve dvou výtiscích, přičemž

každý bude určen pro jednu smluvní stranu. V protokolu bude zřetelně označeno, zda byl předmět plnění (i) akceptován, (ii) akceptován s výhradami, nebo (iii) neakceptován. Pokud bude předmět plnění akceptován Objednatelem s výhradami, nebo nebude akceptován vůbec, bude k protokolu vyhotovena jeho příloha, ve které bude popis výhrad či vad, a bude zde zaznamenán také další dohodnutý postup a termíny odstranění těchto výhrad. Protokol bude podepsán oprávněnou osobou, která provedla na straně Objednatele akceptaci.

5. Před předáním předmětu plnění bude Dodavatel informovat Objednatele o termínu plánovaného předání plnění, a to písemně (alespoň prostřednictvím e-mailu) v dostatečném předstihu tak, aby vzhledem k charakteru předmětu plnění, jeho rozsahu a nárokům na kontrolu a ověření řádnosti a úplnosti jeho poskytnutí byly Objednateli vytvořeny podmínky k tomu, aby provedl kontrolu a ověření bez zbytečného odkladu po předání předmětu plnění Dodavatelem, a provedl akceptaci předmětu plnění ve lhůtě dle čl. IV. odst. 5 této Smlouvy.
6. V případě, že výsledek plnění Dodavatele neobsahuje dle Objednatele žádnou vadu či nedodělek a Objednatel nemá k plnění Dodavatele žádné výhrady ani připomínky, je předmět plnění akceptován bez výhrad, a tato skutečnost bude potvrzena v protokolu o předání a převzetí předmětu plnění.
7. V případě, že výsledek plnění Dodavatele obsahuje dle Objednatele drobné vady či nedodělky, které samostatně ani ve spojení s jinými nebrání užívání předmětu plnění k účelu stanovenému touto Smlouvou, nebo Objednatel má k výsledku plnění Dodavatele nepodstatné výhrady či připomínky, je předmět plnění akceptován s výhradami. Protokolu o předání a převzetí předmětu plnění tak bude obsahovat soupis vytknutých vad, nedodělků, výhrad či připomínek, a také způsoby a přiměřené lhůty pro jejich odstranění, na kterých se smluvní strany dohodly; nedohodnou-li se, budou odstraněny do 5-ti pracovních dnů. Smluvní strany považují v takovém případě výsledek plnění Dodavatele za Dodavatelem řádně předaný a Objednatelem řádně převzatý. Pakliže však nebudou Objednatelem vytknuté vady, nedodělky, výhrady či připomínky odstraněny v souladu se záznamem v protokolu a v termínech v něm uvedených, vzniká Objednateli nárok na smluvní pokutu dle sankčních ustanovení této Smlouvy. Dodavatel písemně informuje Objednatele o odstranění vad, nedodělků, výhrad či připomínek. Objednatel takto doplněný výsledek plnění bez zbytečného odkladu (nejpozději do 3 pracovních dnů od poskytnutí informace Dodavatelem) posoudí, a odstranění vytknutých vad, nedodělků, výhrad či připomínek písemně potvrdí Dodavateli podepsáním přílohy protokolu.
8. V případě, že výsledek plnění Dodavatele trpí jinými než drobnými vadami či nedodělkami, nebo Objednatel má k výsledku plnění Dodavatele podstatné výhrady či připomínky, pak předávaný předmět plnění neakceptuje. Smluvní strany nepovažují v takovém případě výsledek plnění Dodavatele za řádně předaný a Dodavatel je s předáním předmětu plnění v prodlení. Dodavatel je povinen bez zbytečného odkladu odstranit Objednatelem vytknuté vady, nedodělky, výhrady či připomínky, nebo poskytnout nové plnění. O této skutečnosti bude vyhotoven akceptační protokol, avšak v případě neakceptování předmětu plnění je Dodavatel po sjednání nápravy povinen znovu podstoupit celý proces akceptace podle této Smlouvy, aby mohl být předmět plnění Objednatelem akceptován. Tím není dotčena odpovědnost Dodavatele za prodlení s předáním předmětu plnění dle této Smlouvy, ani práva Objednatele z prodlení Dodavatele vyplývající z této Smlouvy.
9. Posouzení skutečnosti, zda vady či nedodělky zjištěné Objednatelem brání užívání předmětu plnění nebo jeho části, náleží výhradně Objednateli. Za vady či nedodělky je pro účely této Smlouvy

10. Při předání předmětu plnění a podpisu protokolu si smluvní strany poskytnou vzájemnou součinnost. K účasti na akceptačním řízení a k podpisu protokolu o předání a převzetí předmětu plnění jsou vedle statutárních zástupců smluvních stran oprávněny tyto osoby:

10.2. na straně Dodavatele

VI. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

1. Ceny plnění dále uvedené v tomto článku Smlouvy jsou cenami úplnými v rozsahu stanoveném přílohou č. 2 této Smlouvy, a zahrnují veškeré náklady Dodavatele k poskytnutí předmětu plnění dle čl. III. odst. 1. a odst. 2. této Smlouvy. Celková cena plnění v uvedeném rozsahu činí:

8.444.106,00 Kč včetně DPH

(slovy: osm milionů čtyři sta čtyřicet čtyři tisíc jedno sto šest korun českých)

2. Celková cena plnění dle předchozího odstavce se sestává z cen za dílčí části plnění, a to ve výši:

- 2.1. Cena za dodávku a implementaci řešení v rozsahu
čl. III. odst. 1. této smlouvy vč. standardní záruky** **5.575.200,00 Kč bez DPH,**

- 2.2. Cena za poskytnutí nadstandardní (prodloužené) záruky 8.300,00 Kč bez DPH,**

- | | |
|---|---------------------------------|
| 2.3. Cena za poskytnutí potřebné maintenance support | |
| a Základní technické podpory na 5 let (1. až 60. měsíc) | 1.395.100,00 Kč bez DPH, |
| 2.3.1. tj. roční plnění maintenance support (12 měsíců) činí | 52.500,00 Kč bez DPH, |
| 2.3.2. tj. roční plnění základní tech. podpory (12 měsíců) činí | 228.000,00 Kč bez DPH, |

3. Výše cen za jednotlivé položky plnění je uvedena v příloze č. 2 této Smlouvy. Za správnost stanovení sazby DPH a výše DPH odpovídá Dodavatel. Sazba DPH a výše DPH bude na faktuře Dodavatele stanovena vždy v aktuálně platné výši.

4. Cena plnění bude hrazena po částech, a to následovně:

- 4.1. Cena dílčí části plnění dle čl. VI. odst. 2.1. této Smlouvy bude uhrazena **jednorázově**, a to po předání a převzetí plnění a podpisu protokolu dle čl. V. odst. 10. této Smlouvy Objednatelem. Datem

uskutečnění zdanitelného plnění je den podpisu protokolu o předání a převzetí předmětu plnění Objednatelem.

- 4.2. Cena dílčí části plnění dle čl. VI. odst. 2.2. této Smlouvy bude uhrazena **jednorázově**, a to po předání a převzetí plnění a podpisu protokolu dle čl. V. odst. 10. této Smlouvy Objednatelem. Datem uskutečnění zdanitelného plnění je den podpisu protokolu o předání a převzetí předmětu plnění Objednatelem.
- 4.3. Cena dílčí části plnění dle čl. VI. odst. 2.3. této Smlouvy bude hrazena postupně **v pravidelných ročních paušálních platbách**, ve výši podílu připadajícího na roční plnění dle odst. 2.3.1. a odst. 2.3.2. tohoto článku Smlouvy, a to pro každý nadcházející rok **předem**. Datem uskutečnění zdanitelného plnění je den výročí zahájení poskytování technické podpory dle této Smlouvy. Pro první rok poskytování technické podpory se za datum uskutečnění zdanitelného plnění považuje první den zahájení poskytování technické podpory následující po předání a převzetí předmětu plnění Objednatelem.
5. Dodavatel vystaví Objednateli daňový doklad (fakturu) na plnění v souladu s odst. 4. tohoto článku Smlouvy. Minimální doba splatnosti faktury vystavené ze strany Dodavatele bude činit 30 dní od doručení faktury Objednateli. Faktura bude splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
6. Dodavatel je povinen vystavit a předat veškeré faktury v elektronickém formátu PDF, a zaslat je datovou zprávou do Datové schránky Objednatele – IDS: x8qbfvu.
7. Nezbytnou přílohou faktury bude zejména soupis skutečně dodaného plnění a provedených prací – zjišťovací protokol. Přílohy budou připojeny v souboru ZIP nebo RAR v pořadí – 1. faktura jako hlavní dokument, 2. přílohy k faktuře jako příloha dokumentu. Plnění či práce, které provedl Dodavatel bez souhlasu Objednatele nad rámec předmětu této Smlouvy, nebudou do soupisu skutečně dodaného plnění a provedených prací zařazeny a považují se za součást celkové ceny, vyjma případů, kdy se smluvní strany písemně dohodnou jinak.
8. Faktura bude nad rámec zákonem požadovaných náležitostí (§ 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty) pro daňový doklad obsahovat také:
 - a) číslo a datum vystavení faktury,
 - b) číslo smlouvy a datum jejího uzavření,
 - c) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření,
 - d) soupis provedených prací včetně zjišťovacího protokolu
 - e) označení banky a číslo účtu, na který musí být zapláceno (pokud je číslo účtu odlišné od čísla uvedeného v této Smlouvě, je Dodavatel povinen o této skutečnosti informovat Objednatele), číslo a datum příslušných akceptačních protokolů podepsaných zástupcem Dodavatele a odsouhlasených zástupcem Objednatele,
 - f) lhůtu splatnosti faktury,
 - g) název, sídlo, IČO a DIČ Objednatele a Dodavatele,
 - h) název a registrační číslo projektu: Zajištění kybernetické bezpečnosti na MěÚ Holešov, reg. č. projektu CZ.31.2.0/0.0/0.0/23_093/0008755,
 - i) jméno a podpis osoby Dodavatele, která fakturu vystavila, včetně kontaktního telefonu.

9. Nebude-li faktura obsahovat zákonem či touto Smlouvou stanovené náležitosti nebo bude chybně vyúčtována cena nebo DPH, je Objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit Dodavateli k provedení opravy s vyznačením důvodu vrácení. Dodavatel provede opravu vystavením nové faktury. Dnem odeslání vadné faktury Objednatelům Dodavateli přestává běžet původní lhůta splatnosti a nová lhůta splatnosti počíná běžet znovu ode dne doručení nové a řádně vystavené faktury Objednateli.
10. V případě prodlení Objednatel se zaplacením řádně vystavené a doručené faktury se Objednatel zavazuje Dodavateli uhradit úrok z prodlení v zákonné výši.
11. Ceny plnění jsou uvedeny jako pevné a nejvýše přípustné ve vztahu k předmětu plnění v rozsahu stanoveném touto Smlouvou k okamžiku jejího uzavření, není-li v této Smlouvě výslovně uvedeno jinak. Smluvní strany sjednaly, že cena plnění zahrnuje rovněž náklady akceptačního řízení, zkušebního či testovacího provozu, technické podpory a servisu, a dalších služeb poskytovaných Dodavatelem Objednateli po dobu trvání této Smlouvy, a rovněž náklady na odstraňování vad a nedodělků plnění a vad plnění v průběhu záruky, včetně odměny za veškeré licence, které byly Objednateli poskytnuty na základě této Smlouvy, není-li dále ujednáno jinak. Dodavatel v souvislosti s ujednáním ceny předmětu plnění na sebe přebírá nebezpečí změny okolností ve smyslu § 2620 odst. 2 občanského zákoníku.
12. V případě, že dojde ke změně zákonné sazby DPH, je Dodavatel k ceně předmětu plnění bez DPH povinen účtovat DPH v platné výši. Tato situace představuje výjimku z nezměnitelnosti ceny předmětu plnění, přičemž smluvní strany výslovně uvádějí, že v případě změny ceny předmětu plnění v důsledku změny sazby DPH nebude ke Smlouvě uzavírán dodatek.
13. Smluvní strany si dále v souladu s § 100 odst. 1 ZZVZ, pro případ trvání a plnění této Smlouvy i po uplynutí prvních 60 měsíců poskytování technické podpory dle čl. III. odst. 2.2. a souvisejících této Smlouvy, vyhrazují právo stanovit pro 6. rok plnění a roky následující způsob stanovení ceny za poskytování technické podpory, a to dle dále uvedených pravidel:
 - 13.1. Výchozí hodnotou je vždy cena za poslední rok poskytování technické podpory (výchozí hodnotou pro stanovení ceny pro 6. rok plnění je tak cena za 5. rok plnění dle čl. VI. odst. 2.3.1. a odst. 2.3.2. této Smlouvy, resp. příslušné položky dle přílohy č. 2),
 - 13.2. Výchozí hodnota může být pro následující rok (12 měsíců) procentuálně zvýšena maximálně o míru inflace v ČR vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen dle údajů publikovaných Českým statistickým úřadem za rok nejbližší předcházející. Ke stanovení hodnoty plnění pro následující rok dojde na základě jednání a souhlasu obou smluvních stran, při respektování maximálního limitu nárůstu dle předchozí věty. Faktické zvýšení hodnoty za poskytování technické podpory bude projevováno ve faktuře vystavené v souladu s odst. 4.3. tohoto článku Smlouvy; uzavření písemného dodatku k této Smlouvě se pro tento případ nevyžaduje.
 - 13.3. Smluvní strany jsou povinny si vzájemně oznámit svůj zájem na pokračování poskytování technické podpory pro každý následující rok plnění nejpozději 6 měsíců před uplynutím aktuálního roku poskytované technické podpory, nebo v téže lhůtě závazek k poskytování technické podpory pro následující rok vypovědět. V případě výpovědi kterékoliv smluvní strany dle předchozí věty zaniknou závazky smluvních stran k poslednímu dni období aktuálního roku poskytované technické podpory.

VII. PRÁVA A POVINNOSTI DODAVATELE, PRAVIDLA VZDÁLENÉHO PŘÍSTUPU DODAVATELE

1. Dodavatel je povinen provést předmět plnění v rozsahu a termínech specifikovaných touto Smlouvou, jejími přílohami, a prováděcím projektem. Zjistí-li Dodavatel překážky, které znemožňují provést předmět plnění dohodnutým způsobem či ve stanovených termínech, je povinen to neprodleně písemně oznámit Objednateli a navrhnout mu změnu v řešení. Jakékoliv změny v řešení, které by vedly ke změně podmínek sjednaných touto Smlouvou, podléhají písemnému schválení Objednatele. Ustanovení § 222 ZZVZ tímto není dotčeno.
2. Dodavatel je povinen provést předmět plnění v souladu s obecně závaznými právními předpisy a v souladu se závaznými interními předpisy Objednatele.
3. Dodavatel je povinen provést předmět plnění řádně a odborně, sám nebo prostřednictvím svých poddodavatelů, které Dodavatel vůči Objednateli identifikuje.
4. Dodavatel není oprávněn postoupit třetí straně jakákoliv práva, nároky či pohledávky plynoucí z této Smlouvy bez předchozího písemného souhlasu Objednatele.
5. Pokud bude při provádění předmětu plnění Dodavatelem využito i volně šiřitelné programové vybavení, je Dodavatel povinen zpracovat přehled licencí a předložit ho jako součást akceptačního protokolu. Dodavatel je povinen zajistit, že poskytnutím uvedených licencí nedojde k porušení práv třetích stran.
6. Dodavatel je povinen určit kontaktní osobu řídící evidenci osob Dodavatele oprávněných k přístupu do síťové infrastruktury Objednatele. V případě změny této kontaktní osoby je Dodavatel povinen bezodkladně oznámit Objednateli takovou změnu, včetně sdělení nové kontaktní osoby.
7. Přístup k síťové infrastruktuře Objednatele je možné povolit pouze po předchozím provedení evidence osoby zastupující Dodavatele v registru identit Objednatele nebo obdobném systému Objednatele, a to na základě požadavku Dodavatele na přístup. Přidělení oprávnění zaměstnancům Dodavatele bude řízeno principem nezbytného minima a není nárokové. Systém pro přístup do síťové infrastruktury Objednatele určí Objednatel.
8. Dodavatel se zavazuje, že neumožní, aby byl tentýž udělený přístup do síťové infrastruktury Objednatele sdílen více zaměstnanci Dodavatele, případně jeho poddodavateli či zaměstnanci poddodavatele.
9. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování předmětu plnění této Smlouvy Objednateli, které přistupují do interní sítě, chránily autentizační prostředky a údaje. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace, a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Dodavatel bere na vědomí, že postup zvládání kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této Smlouvy, a nebude důvodem k jakékoli náhradě případné újmy způsobené Dodavatelem či jiné osobě na jeho straně.
10. Dodavatel se zavazuje, že neumožní připojit koncové zařízení do sítě Objednatele bez předchozího schválení připojení určenou osobu na straně Objednatele.
11. Dodavatel se zavazuje, že všechny jeho informační systémy, které se budou připojovat do síťové infrastruktury Objednatele, jsou a budou chráněny vhodným způsobem proti malware.

12. Dodavatel je povinen mít po celou dobu trvání této Smlouvy zajištěno **pojištění odpovědnosti za škodu** způsobenou třetí osobě, přičemž pojistná částka musí svou výší odpovídat minimálně 6.000.000 Kč. Dodavatel je povinen pojistnou smlouvu, nebo potvrzení o pojištění, předložit Objednateli bezodkladně po uzavření této Smlouvy, nejpozději však do předložení prováděcího projektu před zahájením dodávky a implementace řešení, a dále pak v průběhu provádění předmětu plnění kdykoliv na vyzvání Objednatele.
13. Dodavatel se zavazuje při provádění předmětu plnění dle této Smlouvy zajistit dodržování veškerých pracovněprávních předpisů (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přestávky, legální zaměstnávání pracovníků), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění předmětu této smlouvy podílejí, bez ohledu na to, zda budou činnosti prováděné v rámci plnění předmětu této Smlouvy prováděny přímo Dodavatelem a jeho zaměstnanci, či poddodavatelem. Dodavatel se zavazuje, že provádění předmětu plnění dle této Smlouvy bude prováděno v souladu s úmluvami Mezinárodní organizace práce, jimiž je Česká republika vázána, zejména s úmluvami, které upravují stejné odměňování pracujících mužů a žen za práci stejné hodnoty, diskriminaci, bezpečnost a zdraví pracovníků, a pracovní prostředí.
14. Dodavatel se zavazuje zachovávat férové vztahy ke svým poddodavatelům. Jakýkoliv závazek uzavřený mezi Dodavatelem a jeho poddodavatelem v souvislosti s plněním (částí) předmětu této smlouvy nesmí obsahovat splatnost faktury delší než 30 dnů.
15. Dodavatel se zavazuje při realizaci předmětu této Smlouvy k šetrnému využívání zdrojů a materiálů, k řádnému managementu nakládání s odpady a k omezení jejich nadbytečné produkce.
16. Objednatel je oprávněn průběžně kontrolovat dodržování povinností dodavatele dle odst. 13. až 15. tohoto článku Smlouvy, přičemž Dodavatel je povinen tuto kontrolu umožnit, strpět a poskytnout Objednateli veškerou nezbytnou součinnost k jejímu provedení. Zjistí-li Objednatel, že Dodavatel porušil některou z povinností dle odst. 13. až 15. tohoto článku Smlouvy, a nesjednal nápravu ani po předchozím písemném upozornění Objednatele, je Objednatel oprávněn od této smlouvy odstoupit pro podstatné porušení povinností Dodavatele.

VIII.PRÁVA A POVINNOSTI OBJEDNATELE

1. Objednatel se zavazuje poskytnout Dodavateli součinnost, která je nezbytná k řádnému poskytnutí předmětu plnění této Smlouvy, a lze ji po něm spravedlivě požadovat.
2. Objednatel je oprávněn průběžně vykonávat kontrolu provádění předmětu plnění. Dodavatel umožní provádění kontroly kdykoli během provádění předmětu plnění všem oprávněným osobám určeným Objednatелеm. Dodavatel se též zavazuje předkládat Objednateli na jeho žádost ústní či písemné informace o průběhu a obsahu prováděného plnění, a to nejpozději do 2 (dvou) pracovních dnů od doručení žádosti Objednatele. Pro kontrolu provádění plnění platí:
 - a) Objednatel alespoň 2 (dva) pracovní dny přede dnem plánované kontroly dle přechozího odstavce písemně sdělí Dodavateli termín kontroly. Dodavatel zajistí přítomnost osoby odpovědné za provádění příslušné části předmětu plnění po celou dobu konání kontroly.

- b) O výsledku kontroly smluvní strany provedou písemný zápis ve 2 (dvou) vyhotoveních, každá ze smluvních stran obdrží po 1 (jednom) vyhotovení zápisu.
 - c) Objednatel je oprávněn na základě provedené kontroly požadovat, aby Dodavatel provedl nápravu zjištěného porušení povinnosti Dodavatele nebo odstranění zjištěné vady, a aby plnění poskytoval řádným způsobem.
 - d) Dodavatel za účelem vykonání kontroly poskytne osobě pověřené Objednatелеm výkonem kontroly veškerou nezbytnou součinnost potřebnou pro řádné plnění jejích povinností.
3. Objednatel se zavazuje uhradit Dodavateli řádně a včas veškeré finanční závazky vyplývající z této Smlouvy.

IX. TRVÁNÍ SMLOUVY A UKONČENÍ SMLOUVY

- 1. Smluvní strany se dohodly, že tato Smlouva se sjednává na dobu od okamžiku účinného uzavření této Smlouvy do ukončení technické podpory poskytnutého předmětu plnění.
- 2. Smluvní strany sjednávají poskytování technické podpory předmětu plnění na dobu neurčitou, nebo do doby jejího dřívějšího ukončení podle předchozích ustanovení této Smlouvy nebo podle následujících odstavců tohoto článku Smlouvy.
- 3. Smluvní strany sjednávají možnost předčasného ukončení této Smlouvy písemnou dohodou smluvních stran.
- 4. Smluvní strany se dohodly, že mohou od této Smlouvy odstoupit v případech, kdy to stanoví zákon nebo tato Smlouva. Odstoupení od Smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé smluvní straně. Odstoupením od Smlouvy nezanikají nároky na náhradu škody, smluvní ujednání týkající se volby práva, smluvních pokut, řešení sporů mezi smluvními stranami a jiná ujednání, která podle projevené vůle smluvních stran nebo vzhledem ke své povaze mají trvat i po ukončení Smlouvy. Zejména se jedná o práva a povinnosti související s odpovědností za škodu, smluvními pokutami, fakturací cen, s úroky z prodlení, odpovědností za vady, ochranou osobních údajů a důvěrných informací apod.
- 5. Objednatel je oprávněn odstoupit od této Smlouvy zejména, nikoli však výlučně, v případě, kdy:
 - a) prodlení Dodavatele s předáním předmětu plnění k termínu stanoveném čl. IV. odst. 5. této Smlouvy trvá déle než 15 kalendářních dnů;
 - b) prodlení Dodavatele se splněním povinnosti odstranit vady či nedodělky uvedené v protokolu o předání a převzetí předmětu plnění trvá déle než 7 kalendářních dnů od smluvními stranami sjednaného či Smlouvou stanoveného termínu;
 - c) z průběžně prováděné kontroly vyvstanou důvodné pochybnosti o schopnosti Dodavatele splnit předmět plnění řádně a úplně, a Dodavatel nebude schopen na výzvu Objednatele tyto objektivní důvody vyvrátit;
 - d) předmět plnění vykazuje vady či nedodělky, které neumožní jeho řádné užívání k účelu, který je sjednán touto Smlouvou,
 - e) prokáže-li se kterékoliv prohlášení Dodavatele učiněné v této Smlouvě jako nepravdivé,
 - f) Dodavatel neplní pokyny Objednatele při poskytování předmětu plnění, a nezjedná nápravu do 7

kalendářních dnů poté, co byl Objednatelem na tuto skutečnost písemně upozorněn,

- g) Dodavatel brání Objednateli v provádění kontrol či zkoušek předmětu plnění nebo jeho částí, či více než 7 kalendářních dnů neposkytuje součinnost, ke které se zavázal touto Smlouvou,
 - h) pokud Dodavatel nevyhoví požadavku Objednatele na výměnu poddodavatele, pokud byly splněny podmínky podle této Smlouvy,
 - i) poruší-li Dodavatel opakovaně (více než dvakrát) pravidla pro vzdálený přístup Dodavatele stanovená v čl. VII. této Smlouvy nebo nezajistí-li jejich dodržování,
 - j) v případech vymezených § 223 odst. 1 až 3 ZZVZ,
 - k) dostane-li se Dodavatel do stavu úpadku nebo hrozícího úpadku, dojde-li k zahájení likvidace Dodavatele, nebo dojde-li k poškození podstatné části majetku Dodavatele výkonem rozhodnutí nebo exekucí.
6. Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 kalendářních dnů, pokud Objednatel nezjedná nápravu ani v dodatečně přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 15 kalendářních dnů od prokazatelného doručení takovéto výzvy Objednateli. Toto ustanovení se dle dohody smluvních stran nevztahuje na případy, kdy bude prodlení Objednatele zapříčiněno opožděným uvolněním finančních prostředků z veřejných zdrojů.
7. V případě odstoupení od Smlouvy nemá Dodavatel nárok na zaplacení ceny předmětu plnění v plném rozsahu. Dodavatel je pouze oprávněn žádat po Objednateli to, o co se Objednatel poskytnutím předmětu plnění Dodavatelem obohatil, a to v rozsahu plnění, které je Objednatelem využitelné i po takovém odstoupení od Smlouvy.
8. Smluvní strany se dohodly, že v případě předčasného ukončení Smlouvy odstoupením od Smlouvy si poskytnou vzájemnou součinnost k převodu a nabytí licencí či oprávnění plynoucích z takových licencí již pořízených Dodavatelem pro Objednatele, kterými Objednatel nedisponuje, resp., které Objednatel případně dosud neuhradil Dodavateli podle čl. VI. této Smlouvy. Dodavatel je povinen takové licence převést na Objednatele, a Objednatel je povinen je nabýt a uhradit za ně Dodavateli cenu stanovenou podle této Smlouvy, celkově nejvýše však do částky odpovídající výši platby za 1 rok, nebrání-li takovému převodu objektivní překážky ležící vně vůle smluvních stran.
9. Při předčasném ukončení závazku z této Smlouvy se Dodavatel zavazuje provést na své náklady veškeré práce, které budou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či na straně třetích osob. Dodavatel bude v takovém případě rovněž povinen předat Objednateli bezplatně veškeré informace, které s dílem souvisí a jsou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či třetích osob.

X. REALIZAČNÍ TÝM

1. Dodavatel provede předmět plnění zejména prostřednictvím osob, které jsou uvedeny v příloze č. 3 této Smlouvy. Jedná se o osoby, kterými Dodavatel prokazoval splnění části technické kvalifikace v rámci své účasti v zadávacím řízení veřejné zakázky.

2. Dodavatel prohlašuje, že se všichni členové realizačního týmu, jimiž v rámci zadávacího řízení veřejné zakázky prokazoval splnění kvalifikace, budou aktivně podílet na provedení příslušné části předmětu plnění podle této Smlouvy a nabídky podané v rámci zadávacího řízení veřejné zakázky.
3. V případě, že kvalita předmětu plnění dle této Smlouvy prováděná některým z členů realizačního týmu neodpovídá požadavkům této Smlouvy, nebo člen realizačního týmu nevykonává pokyny Objednatele podle Smlouvy, nebo nastane jiný závažný důvod pro změnu realizačního týmu, pak je Objednatel oprávněn požadovat výměnu člena realizačního týmu. Dodavatel do 10 kalendářních dnů od doručení žádosti Objednatele navrhne nového člena realizačního týmu, přičemž nově navržený člen realizačního týmu musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval původní člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizačního týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní. Nový člen realizačního týmu následně musí být akceptován ze strany Objednatele. Akceptace nového člena realizačního týmu je podmíněna předložením dokladů, prokazujících dosažení minimálně shodné úrovně jeho zkušeností jako u původního člena.
4. Pokud jsou důvody pro změnu některého ze členů realizačního týmu dány na straně Dodavatele, Dodavatel může ke změně přistoupit pouze ze závažných důvodů s předchozím souhlasem Objednatele. Nově navržený člen realizačního týmu přitom musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizačního týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní. Objednatel udělí písemný souhlas se změnou do 10 kalendářních dnů od doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující dosažení minimálně shodné úrovně zkušeností nového člena jako u původního člena.
5. Realizační tým Dodavatele může být tvořen i dalšími osobami nad rámec počtu stanoveného minimálními požadavky kvalifikace. Dodavatel se zavazuje, že při běžné pracovní komunikaci s Objednatelem či jeho zástupci bude užíváno českého nebo slovenského jazyka, nedohodnou-li se smluvní strany či jejich jednotliví zástupci jinak.

XI. PODDODAVATELÉ

1. Dodavatel je oprávněn využít k provedení předmětu plnění jiné osoby pouze v případě, že tyto osoby jsou součástí seznamu poddodavatelů, který tvoří přílohu č. 4 této Smlouvy a který byl rovněž součástí nabídky Dodavatele do veřejné zakázky, není-li stanoveno jinak. Dodavatel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení veřejné zakázky, se budou podílet na plnění povinností Dodavatele vyplývajících ze Smlouvy v rozsahu podle nabídky Dodavatele podané do zadávacího řízení veřejné zakázky.
2. Dodavatel odpovídá za plnění poddodavatele tak, jako by plnil sám. Dodavatel je povinen vybrat takového poddodavatele, který neodporuje požadavkům, jaké má Objednatel na Dodavatele.
3. Dodavatel prohlašuje a zavazuje se, že ručí za uspokojení povinností poddodavatele nahradit újmou způsobenou poddodavatelem Objednateli při plnění nebo v souvislosti s plněním povinností ze Smlouvy, jestliže povinnost k náhradě újmy nesplnil poddodavatel sám.

4. V případě, že poddodavatel je s plněním svých závazků, které přímo souvisí s předmětem této smlouvy, v prodlení více než 10 kalendářních dnů, nebo byl poddodavatel uložen zákaz plnění veřejných zakázek, ocitnul se v úpadku nebo hrozícím úpadku, nebo byl pravomocně odsouzen za trestný čin uvedený v příloze č. 3 ZZVZ, nebo je zde jiný vážný důvod, pak je Objednatel oprávněn požadovat po Dodavateli výměnu poddodavatele. Za jiný vážný důvod dle předchozí věty se považuje rovněž stav nerefluktování výhrad sdělených Objednatel k činnosti poddodavatele, či řádnosti a kvality jím poskytovaného plnění apod., kdy uvedené nedostatky nebyly napraveny ani po předchozí písemné stížnosti adresované Objednatel Dodavateli. Dodavatel je povinen navrhnout nového poddodavatele do 10 kalendářních dnů od doručení žádosti Objednatele. Nový poddodavatel se může podílet na poskytování předmětu plnění pouze na základě písemného souhlasu Objednatele, který Objednatel udělí po provedení kontroly dokladů předložených Dodavatelem k novému poddodavatel.
5. Pokud jsou důvody pro změnu či doplnění poddodavatele dány na straně Dodavatele, Dodavatel může ke změně či doplnění přistoupit pouze s předchozím souhlasem Objednatele. Jedná-li se o změnu poddodavatele, prostřednictvím něhož byla prokazována kvalifikace, nově navržený poddodavatel musí disponovat stejnou nebo vyšší úroveň kvalifikace, jakou disponoval poddodavatel, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky. Objednatel udělí písemný souhlas se změnou poddodavatele po doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující kvalifikaci nového poddodavatele, a po provedení kontroly takto předložených dokladů.

XII. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA, DUŠEVNÍ VLASTNICTVÍ

1. Objednatel nabývá vlastnické právo k poskytnutému předmětu plnění podpisem akceptačního protokolu, a to v rozsahu akceptace.
2. Dodavatel se zavazuje při poskytování předmětu plnění neporušit práva třetích osob, která těmto osobám mohou plynout z duševního vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Dodavatel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku uplatnění práv třetích osob vůči Objednateli v souvislosti s porušením povinnosti Dodavatele dle předchozí věty. Uplatní-li třetí osoba své právo k předmětu plnění nebo jeho části, zavazuje se Dodavatel dále Objednateli bezplatně poskytnout, zabezpečit a/nebo uhradit náhradní řešení, které nebude dotčeno právem třetí osoby.
3. V případě, že je výsledkem činnosti Dodavatele dle této Smlouvy či jeho součástí dílo, které podléhá ochraně podle zákona č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně dalších zákonů (autorský zákon), v platném znění (dále jen „autorský zákon“) a občanského zákoníku, získá Objednatel k takto vytvořenému dílu jako celku i k jeho jednotlivým částem licenci, přičemž odměna za poskytnutou licenci je již součástí ceny předmětu plnění.
4. Pro účely této Smlouvy rozlišují smluvní strany mezi „Individualizovaným dílem“ a „Standardizovaným dílem“, kdy:
 - Individualizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které bylo vytvořeno nebo upraveno pro účely této Smlouvy;
 - Standardizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které nebylo vytvořeno nebo upraveno pro účely této Smlouvy.

V případě pochybností se na plnění hledí jako na Individualizované dílo, dokud Dodavatel neprokáže opak.

5. Dodavatel na základě této Smlouvy poskytuje Objednateli oprávnění k výkonu práv duševního vlastnictví k Individualizovanému dílu. Licence se týká veškerých autorských nebo jiných duševních práv k Individualizovanému dílu, jejichž povaha umožňuje licenci v dále uvedeném rozsahu poskytnout, a to:
 - a) licence k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně, k účelu stanovenému touto Smlouvou a v rozsahu minimálně nezbytném pro řádné užívání příslušného Individualizovaného díla Objednatelům v souladu s touto Smlouvou;
 - b) licence neodvolatelná a nevypověditelná;
 - c) licence neomezená územním rozsahem a rovněž tak neomezená způsobem nebo rozsahem užití;
 - d) licence udělená na dobu určitou, a to po celou dobu trvání majetkových práv k dílu (účinnost licence však trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak);
 - e) licence vztahující se i na budoucí aktualizace dodaného předmětu plnění v rámci jeho podpory;
 - f) licence převoditelná a postupitelná, tj. která je udělena s právem udělení podlicence či postoupení licence jakékoliv třetí osobě;
 - g) licence, kterou není Objednatel povinen využít.
6. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy. Dodavatel podpisem Smlouvy prohlašuje, že vlastní či oprávněně disponuje veškerými oprávněními k autorskému dílu, které bude součástí předmětu plnění dle této Smlouvy, zejména, nikoliv však výlučně, že získal veškerá oprávnění autorů či třetích osob k takovému dílu a je oprávněn je poskytnout Objednateli, a to zejména, nikoliv však výlučně, veškerá oprávnění uvedená v tomto článku Smlouvy.
7. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel (či jím pověřená třetí osoba) dle své potřeby zasahoval do Individualizovaného díla, zejm. je oprávněn jej zveřejnit, upravovat, zpracovávat, překládat, měnit jeho název, spojit s dílem jiným a zařadit jej do díla souborného. Ustanovení tohoto odstavce neomezuje práva Objednatelů plynoucí z § 66 zákona č. 121/2000 Sb., autorský zákon.
8. Dodavatel se zavazuje zajistit oprávnění k užití předmětu práv duševního vlastnictví jiných osob, který představuje Individualizované dílo, a souhlas se zásahy do takového předmětu práv duševního vlastnictví v takovém rozsahu, aby Objednateli mohl udělit licenci k Individualizovanému dílu v rozsahu této Smlouvy, souhlas k zásahům ve smyslu předchozího odst. 7. tohoto článku Smlouvy, a aby mohl Objednateli předat zdrojový kód a dokumentaci k takovému předmětu práv duševního vlastnictví.
9. Jedná-li se o oprávnění k výkonu práv duševního vlastnictví ke Standardizovanému dílu, je Dodavatel povinen Objednateli poskytnout:
 - a) licenci ke Standardizovanému dílu, pokud je autorem Standardizovaného díla Dodavatel, nebo
 - b) zajistit poskytnutí licence ke Standardizovanému dílu Objednateli třetí osobou, pokud je autorem Standardizovaného díla jiná třetí osoba,a to v rozsahu, který zajistí plnou využitelnost Standardizovaného díla při jeho vývoji, rozvoji, provozu a užívání bez nutnosti platit Dodavateli nebo třetí osobě odměnu nad rámec odměny dle této Smlouvy. Nabyvatelem licence ke Standardizovanému dílu podle tohoto odstavce musí být bezprostředně Objednatel.

10. Dodavatel je při plnění této Smlouvy oprávněn použít tzv. free and open-source software (dále jen „FOSS“) s tím, že užití FOSS a licence se k tomu vztahující nesmí být v rozporu s účelem této Smlouvy. Dodavatel společně s předáním svého výstupu, který obsahuje FOSS, sdělí Objednateli informace o tom, že byl FOSS použit a jaké licenční podmínky se na užití FOSS vztahují. Využije-li Dodavatel při plnění této Smlouvy FOSS, zavazuje se zajistit po dobu trvání Smlouvy jeho podporu tak, aby nedošlo k omezení jeho funkčnosti či bezpečnosti, zejména v situaci, kdy původní tvůrce příslušného FOSS ukončí poskytování podpory. Odměna za jakékoliv plnění Dodavatele související se zajištěním podpory FOSS dle předchozí věty, včetně případného nahrazení FOSS bez podpory jiným software, je zahrnuta v odměně za poskytování technické podpory dle čl. VI. této Smlouvy a Dodavateli nenáleží žádná další odměna či kompenzace.
11. Dodavatel je povinen současně s předáním předmětu plnění, resp. těch částí předmětu plnění, které jsou počítačovým programem, předat Objednateli zdrojový kód včetně administrátorského přístupu k němu (dále jen „zdrojový kód“); výjimku z této povinnosti tvoří odst. 14. tohoto článku Smlouvy.
12. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace zdrojového kódu, na základě které bude Objednatel schopen zjistit veškeré funkce a vnitřní vazby počítačového programu a zasahovat do něj. Zdrojový kód bude Objednateli Dodavatelem předán na nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód“ a označením jeho verze a dne předání zdrojového kódu, případně na základě dohody smluvních stran bude k předání využito sdíleného elektronického úložiště, které zřídí Dodavatel a poskytne do něj Objednateli přístup. O předání zdrojového kódu bude smluvními stranami sepsán písemný protokol.
13. Povinnost Dodavatele uvedená v předcházejícím odstavci se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu, k nimž dojde při provádění předmětu plnění nebo v rámci jeho oprav (dále jen „změna zdrojového kódu“). Dokumentace změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.
14. Výjimkou z ujednání týkajících se předání zdrojového kódu je situace, kdy součástí plnění je Standardizované dílo a předání zdrojového kódu ke Standardizovanému dílu není možné s ohledem na práva třetích osob.
15. Práva získaná v rámci plnění poskytnutého podle tohoto článku Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.

XIII. ODPOVĚDNOST ZA VADY, ZÁRUKA A TECHNICKÁ PODPORA

1. Dodavatel poskytuje záruku za dodané řešení v délce, která je pro jednotlivé součásti řešení uvedena v příloze č. 1 této Smlouvy, minimálně však standardní záruku po dobu prvních 36 měsíců od převzetí dokončeného řešení Objednatelem, a dále nadstandardní (prodlouženou) záruku v délce 24 měsíců následujících po uplynutí standardní záruky, celkem tedy 60 měsíců.
2. Dodavatel odpovídá za vady, které má předmět plnění v době jeho převzetí a akceptace, a za vady, které se projeví v záruční době, popřípadě v důsledku škody, za kterou odpovídá Dodavatel.

3. Veškeré vady předmětu plnění je Objednatel oprávněn uplatnit u Dodavatele kdykoliv po zjištění vady během záruky, a to formou písemného oznámení, obsahujícího specifikaci zjištěné vady nebo popis, jak se vada projevuje. Objednatel je oprávněn uplatnit veškerá zákonná práva z vadného plnění. Volba práva z vadného plnění svědčí Objednateli. Neuvede-li Objednatel, jaké právo v souvislosti s vadou předmětu plnění uplatňuje, má se za to, že požaduje odstranění vady, tj. provedení opravy předmětu plnění nebo jeho části.
4. Dodavatel v rámci předmětu plnění této Smlouvy poskytuje Objednateli rovněž technickou podporu daného řešení. Toto plnění zahrnuje zejména (nikoli výlučně):
 - odstraňování nebo spolupráci při odstraňování závad či nefunkčností,
 - kontrolu stavu jednotlivých komponent řešení a po vzájemné dohodě aplikaci nápravných opatření,
 - řešení vzniklých problémů a incidentů,
 - bezplatná výměna vadného zařízení/komponentu,
 - aktualizace firmware a software dodaných produktů,
 - aktualizaci dokumentace,
 - na vyžádání změnu nastavení, konfiguraci řešení,
 - podporu při implementaci upgradů,
 - poskytování informací,
 - poskytování odborných konzultací a podpory.
5. Za účelem poskytování služeb technické podpory a příjmu požadavků Objednatele je Dodavatel povinen zřídit a udržovat po celou dobu trvání této Smlouvy systém HelpDesk. Systém HelpDesk bude dostupný na adrese: <https://acservicedesk.autocont.cz>.
6. Příjem požadavků v systému HelpDesk musí být zajištěn v režimu 7x24x365. Samotná technická podpora Dodavatele bude poskytována v pracovní dny v pracovní době od 07:00 do 17:00 hodin (dále jen „pracovní doba“).
7. Garantovaná doba odezvy Dodavatele na Objednatelem nahlášený požadavek v systému HelpDesk činí v rámci pracovní doby 1 hodinu. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem shora uvedené doby 07:00 hodin nejbližšího pracovního dne.
8. Dodavatel je povinen zahájit řešení **kritického incidentu** ohrožujícího provoz nejpozději do 2 pracovních hodin od nahlášení požadavku v systému HelpDesk, a v případě **nekritického incidentu** NBD (next business day) od nahlášení.
9. Dodavatel je povinen vyřešit požadavek za podmínek stanovených v příloze č. 1 této Smlouvy ve lhůtě dohodnuté zástupci Objednatele a Dodavatele, a nedohodnou-li se, pak v případě kritického incidentu ve lhůtě nejpozději do 1 pracovního dne od nahlášení, a v případě nekritického incidentu do 2 pracovních dnů od nahlášení požadavku v systému HelpDesk. V případě kritických incidentů způsobujících nefunkčnost řešení se Dodavatel zavazuje vyvinout maximální úsilí k odstranění závady způsobující takovou nefunkčnost a tuto odstranit bez zbytečného odkladu v co nejkratší technicky obhajitelné lhůtě.
10. Technická podpora bude Dodavatelem poskytována jak proaktivně (např. průběžné kontroly stavu komponent Dodavatelem), tak reaktivně (činnost Dodavatele vyvolaná na základě žádosti Objednatele). Kontaktními osobami v záležitostech poskytování technické podpory jsou:

10.1. na straně Objednatele: [REDACTED]

10.2. na straně Dodavatele: [REDACTED]

11. Dodavatel je povinen vést evidenci poskytování technické podpory a předkládat ji Objednateli pravidelně 1 x za čtvrtletí, nebo na žádost Objednatele mimo uvedený interval (dále jen „reporty“). Z reportů bude zřejmé, v jakém rozsahu a v jaké oblasti byly služby technické podpory poskytnuty, a jaká je bilance čerpání hodin základní technické podpory. Nespotřebované hodiny základní technické podpory za jednotlivé měsíce jsou převoditelné v rámci jednoho roku. Dodavatel se zavazuje, že umožní Objednateli přístup k evidenci požadavků v HelpDesku Dodavatele a uchová takto přístupné záznamy po dobu trvání této Smlouvy, minimálně do ukončení poskytování technické podpory.
12. Další podmínky poskytování technické podpory jsou uvedeny v příloze č. 1 této Smlouvy.

XIV. NÁHRADA ŠKODY

1. Každá smluvní strana je povinna nahradit škodu jí způsobenou dle platných právních předpisů a této Smlouvy. Obě smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
2. V případě, že při činnosti prováděné Dodavatelem dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním Dodavatele sjednaným dle této Smlouvy, bude Dodavatel povinen tuto škodu uhradit z vlastních prostředků.
3. Pokud v důsledku porušení povinností Dodavatele stanovených touto Smlouvou nebude Objednateli uhrazen finanční podíl nebo jeho část poskytovatelem dotace na projektu „Zajištění kybernetické bezpečnosti na MěÚ Holešov“, reg. č. projektu CZ.31.2.0/0.0/0.0/23_093/0008755, bude Dodavatel povinen uhradit Objednateli takto způsobenou škodu (celý finanční podíl, který nebude poskytovatelem dotace podle jeho rozhodnutí vyplacen, nebo který bude muset být Objednatelem vrácen).

XV. SANKCE

1. V případě prodlení Dodavatele s předáním předmětu plnění ve lhůtě dle čl. IV. odst. 5. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 0,2 % z ceny za dodávku a implementaci řešení dle čl. VI. odst. 2.1. této Smlouvy za každý den prodlení Dodavatele.
2. V případě prodlení Dodavatele se splněním dílčího termínu dle čl. IV. odst. 3 této Smlouvy (T1, T2, T3, T4), sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 1.000 Kč za každý den prodlení Dodavatele.
3. V případě prodlení Dodavatele se splněním povinnosti odstranit vady uvedené v protokolu o předání a převzetí plnění v ujednané lhůtě, včetně drobných vad předmětu plnění, které byly Objednatelem vytknuty, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý i započatý den a za každý případ prodlení (za každou vadu).

4. V případě prodlení Dodavatele s předáním zdrojového kódu, dokumentace nebo jiných souvisejících věcí dle čl. XII. odst. 11. a odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení.
5. V případě prodlení Dodavatele se splněním povinnosti zahájit řešení požadavku nahlášeného Objednatelem ve lhůtě dle čl. XIII. odst. 8. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 1.000 Kč za každou i započatou hodinu prodlení v rámci pracovní doby Dodavatele.
6. V případě prodlení Dodavatele se splněním povinnosti vyřešit Objednatelem nahlášený požadavek ve lhůtě stanovené dle čl. XIII. odst. 9. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý pracovní den prodlení Dodavatele.
7. V případě nesplnění povinnosti Dodavatele vést evidenci poskytování technické podpory nebo v případě prodlení s jejím předložením Objednateli sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý jednotlivý případ.
8. V případě:
 - a) porušení povinností Dodavatele v souvislosti s užívacími právy dle této Smlouvy sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti, nestanoví-li Smlouva pro určité porušení jinou smluvní pokutu;
 - b) porušení povinností Dodavatele vztahujících se k ochraně osobních údajů vymezených v této Smlouvě, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti;
 - c) porušení povinnosti mlčenlivosti a ochrany důvěrných informací, či podmínek a požadavků na zajištění kybernetické bezpečnosti vymezených v této Smlouvě Dodavatelem, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 200.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti. Za porušení povinnosti mlčenlivosti ze strany Dodavatele jsou pro účely této Smlouvy považovány i případy, kdy k porušení mlčenlivosti dojde ze strany osob, které se podílely na poskytování předmětu plnění vůči Objednateli;
9. V případě, že Dodavatel poruší své povinnosti ve vztahu k pracovněprávní ochraně svých zaměstnanců nebo zaměstnanců poddodavatele, sjednávají smluvní strany povinnost Dodavatele zaplatit Objednateli smluvní pokutu ve výši 1.000 Kč za každý zjištěný případ.
10. V případě, že Dodavatel nedodrží svou povinnost ve vztahu k pravidlům pro vzdálený přístup Dodavatele stanoveným v čl. VII. odst. 6., odst. 7., odst. 8., odst. 10. a odst. 11. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 3.000 Kč za každý jednotlivý zjištěný případ porušení této povinnosti.
11. V případě, že Dodavatel nedodrží svou povinnost předložit Objednateli kopii pojistné smlouvy nebo nebude udržovat své pojištění za podmínek stanovených v čl. VII. odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení, ve kterém nebude uvedená povinnost Dodavatele splněna.

12. Smluvní pokuty a/nebo úroky z prodlení jsou splatné na bankovní účet oprávněné smluvní strany do 14 kalendářních dnů ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší.
13. Úhrada jakékoliv smluvní pokuty nezavazuje Dodavatele povinnosti splnit své závazky ze Smlouvy, ani jí není dotčen nárok Objednatele na náhradu škody v plné výši, ani povinnost Dodavatele bezodkladně odstranit závadný stav.

XVI. OCHRANA OSOBNÍCH ÚDAJŮ

1. Dodavatel prohlašuje, že si je vědom, že Objednatel jako správce osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) zpracovává osobní údaje Dodavatele, jeho zaměstnanců či členů orgánů a osobní údaje poddodavatelů Dodavatele, jejich zaměstnanců a členů orgánů (vše společně dále jen „osobní údaje“) pro účely plnění povinností vyplývajících ze zákona, plnění závazků podle této Smlouvy nebo oprávněných zájmů Objednatele.
2. Objednatel prohlašuje, že veškeré osobní údaje, které Dodavatel poskytne Objednateli nebo se kterými přijde Objednatel do styku v souvislosti s plněním závazku podle této Smlouvy, nebudou využívány k jiným účelům, než k jakým byly Dodavatelem Objednateli poskytnuty nebo Objednatelem pro účely plnění této Smlouvy shromážděny.
3. Dodavatel se zavazuje chránit veškeré osobní údaje, které mu budou poskytnuty, zpřístupněny či se kterými přijde do styku v souvislosti s plněním předmětu této Smlouvy.

XVII. OCHRANA INFORMACÍ, KYBERNETICKÁ BEZPEČNOST

1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:
 - a) si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“);
 - b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejím opomenutím přístup k důvěrným informacím a osobním údajům druhé smluvní strany.
2. Smluvní strany se zavazují, že žádná z nich bez písemného souhlasu druhé smluvní strany nezpřístupní třetí osobě důvěrné informace, které získala při plnění této Smlouvy, ani je nepoužije v rozporu s účelem této Smlouvy.
3. Veškeré informace, které Dodavatel při plnění této Smlouvy získá od Objednatele nebo o Objednateli či jeho zaměstnancích a spolupracovnících, se považují za důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Dodavatelem Objednateli se považují za důvěrné, pouze pokud na jejich důvěrnost Dodavatel Objednateli předem písemně upozornil a Objednatel Dodavateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat.

4. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak než za účelem plnění této Smlouvy.
5. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel povinen uveřejnit na příslušných webových stránkách v souladu se ZZVZ či 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) tuto Smlouvu včetně všech jejích změn a dodatků;
 - b) výši skutečně uhrazené ceny za plnění veřejné zakázky.
6. Dodavatel se zavazuje k zachování bezpečnosti informací a dat obsažených v informačních systémech spravovaných Objednatelem, včetně jiných informačních systémů, které budou plněním smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Dodavatel je povinen při provádění díla jednat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla přerušena, ohrožena, ani omezena. Je-li k plnění dle smlouvy nezbytné důvěrnost, dostupnost či integritu dat omezit, ohrozit nebo přerušit, Dodavatel tak učiní pouze po předchozí dohodě s Objednatelem a jen v Objednatelem odsouhlaseném rozsahu.
7. Dodavatel je povinen v průběhu realizace plnění dle této Smlouvy průběžně poskytovat součinnost při identifikaci významných změn a jejich dopadů do oblasti kybernetické bezpečnosti Objednatele. V případě identifikace významných změn souvisejících s realizací plnění se Poskytovatel zavazuje spolupracovat s Objednatelem na identifikaci potenciálních rizik možných dopadů významných změn a v případě potřeby poskytne Objednateli informace o možných opatřeních pro snížení nepříznivých možných dopadů spojených s významnými změnami.
8. V případě výskytu kybernetického bezpečnostního incidentu, který souvisí s realizací plnění, je Dodavatel povinen o něm Objednatele neprodleně písemně informovat, a to nejpozději do následujícího dne po zjištění kybernetického bezpečnostního incidentu. Toto hlášení bude identifikovat konkrétní část předmětu plnění, kde ke kybernetickému bezpečnostnímu incidentu došlo, dále sdělení, kdy k němu došlo, a zejména popis tohoto incidentu. Smluvní strany následně budou spolupracovat na řešení incidentu a na nápravných opatřeních, tak aby byla minimalizována rizika z incidentu vyplývající.
9. Dodavatel se bude řídit bezpečnostní politikou a předpisy Objednatele, se kterými byl Objednatelem seznámen a které souvisí s plněním dle smlouvy.

XVIII. SOUČINNOST A EXTERNÍ KONTROLA

1. Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.

2. Dodavatel uchová veškerou dokumentaci a účetní doklady související s plněním podle této Smlouvy minimálně do 31.12.2036. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být použita pro úschovu delší lhůta, a to i delší než lhůta ujednaná tímto odstavcem Smlouvy.
3. Dodavatel je povinen minimálně do 31. 12. 2036 poskytovat sám či prostřednictvím Objednatele požadované informace a dokumentaci (včetně účetních dokladů) související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (OLAF – Evropský úřad pro boj proti podvodům, Úřad evropského veřejného žalobce, Ministerstva financí ČR, Evropské komise, Evropského účetního dvora, Ministerstva vnitra ČR, Nejvyššího kontrolního úřadu a dalším příslušným vnitrostátním orgánům), a je povinen vytvořit výše uvedeným subjektům podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost. Náklady související s těmito kontrolami a poskytováním informací a součinnosti jsou zahrnuty do ceny díla.

XIX. ROZHODNÉ PRÁVO

1. Vztahy mezi smluvními stranami touto Smlouvou výslovně neupravené se budou řídit obecně závaznými právními předpisy České republiky, zejména občanským zákoníkem a příslušnými právními předpisy souvisejícími.
2. Veškeré spory mezi smluvními stranami vyplývající z této Smlouvy nebo z jejího porušení, ukončení nebo neplatnosti budou rozhodovány věcně a místně příslušnými soudy České republiky dle sídla Objednatele, pokud nebudou vyřešeny dohodou obou smluvních stran.

XX. ZÁVĚREČNÁ USTANOVENÍ

1. Tato Smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti nabývá okamžikem zveřejnění Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel.
2. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků této Smlouvy uzavřených v souladu s příslušnými ustanoveními občanského zákoníku, popř. obdobných předpisů tyto předpisy nahrazujících, a podepsaných osobami oprávněnými jednat jménem smluvních stran.
3. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této Smlouvy byla jakákoliv práva a povinnosti dovozována z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklosti zachovávaných obecně či v odvětví týkajícím se předmětu plnění této Smlouvy, ledaže je v této Smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
4. Smluvní strany se podpisem této Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 občanského zákoníku.
5. Pro vyloučení pochybností Dodavatel výslovně potvrzuje, že je podnikatelem, uzavírá tuto Smlouvu při svém podnikání, a na tuto Smlouvu se tudíž neuplatní ustanovení § 1793 občanského zákoníku.

6. Dodavatel na sebe v souladu s ustanovením § 1765 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva smluvních stran upravená v této Smlouvě.
7. Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení této Smlouvy. Smluvní strany se tímto zavazují nahradit do 10-ti pracovních dnů po doručení výzvy druhé smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.
8. Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce smluvních stran.
9. Dodavatel není oprávněn započítat, zastavit ani postoupit žádné své peněžité nároky vůči Objednateli vzniklé na základě této Smlouvy na třetí osobu bez předchozího písemného souhlasu Objednatele.
10. Dodavatel se zavazuje, že bez předchozího výslovného písemného souhlasu Objednatele nepostoupí třetí straně tuto Smlouvu nebo jakoukoli její část nebo jakékoli právo či závazek z této Smlouvy vyplývající. Toto ustanovení se nevztahuje na případné právní nástupce smluvních stran.
11. Tato Smlouva je uzavřena elektronickou formou s využitím kvalifikovaných elektronických podpisů osob oprávněných právně jednat v zastoupení smluvních stran.
12. Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a na důkaz dohody o všech článcích této Smlouvy připojují své podpisy.
13. Nedílnou součástí této Smlouvy jsou:
- Příloha č. 1 – Technická specifikace a popis nabízeného řešení
- Příloha č. 2 – Cenová nabídka
- Příloha č. 3 – Realizační tým
- Příloha č. 4 – Seznam poddodavatelů
14. Doložka právního jednání podle § 41 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů:
- Rozhodnuto orgánem obce: Radou města Holešova dne 25.06.2025.
- Datum a číslo jednací: 267/13/RM/2025.

Za Objednatele

Za Dodavatele

V Holešově

V Ostravě

Mgr.
Milan Fritz

Digitálně podepsal
Mgr. Milan Fritz
Datum: 2025.07.03
11:13:45 +02'00'

Mgr. Milan Fritz
starosta

Ing.
Jaroslav
Dvořák

Digitálně
podepsal Ing.
Jaroslav Dvořák
Datum:
2025.07.01
19:06:05 +03'00'

Jaroslav Dvořák
člen představenstva

Tomáš
Ječmínek

Digitally signed
by Tomáš
Ječmínek
Date: 2025.07.01
18:41:49 +02'00'

Tomáš Ječmínek
člen představenstva



Město Holešov

TECHNICKÁ SPECIFIKACE

KYBERBEZPEČNOST



**Národní
plán
obnovy**



**Financováno
Evropskou unií
NextGenerationEU**



**MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY**

Veškeré produkty, které dodavatel dodává v rámci plnění zadavatel, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

- (a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
- (b) mají plnou záruku od výrobce,
- (c) jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
- (d) obsahují všechny nezbytné licence na používání příslušného softwaru,
- (e) jsou určeny pro provoz v České republice (EU).

Tyto skutečnosti dodavatel doloží:

- a) potvrzením výrobce daného zařízení, nebo
- b) čestným prohlášením distributora, nelze-li prohlášení výrobce získat, nebo
- c) jiným rovnocenným dokladem (doklady) v případě, že doklady dle předchozích písm. a) a b) není dodavatel z důvodů, které mu nelze přičítat, schopen předložit (takové důvody musí dodavatel doložit).

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení dle předchozího odstavce ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

1) Nástroj pro zajišťování úrovně dostupnosti informací

- **Server 2 ks**
- **Server OS + CAL**
- **Software Defined Storage**

2) Nástroj pro ochranu integrity komunikačních sítí

3) Systém pro analýzu síťového provozu a bezpečnostní monitoring

4) NAS - Network Attached Storage

5) Nástroj pro ochranu koncových stanic

6) Nástroj pro ověřování identity uživatelů

7) Nástroj pro ochranu a zabezpečení e-mailů

8) Nástroj pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

9) Ochrana počítačové sítě před malwarem a zneužíváním zařízení na úrovni DNS překladu, řešení poskytujícího plnou kontrolu nad DNS provozem

1) Nástroj pro zajišťování úrovně dostupnosti informací

Server 2 ks

Parametr	Minimální požadavek
Výrobce a model	2x HPE DL380 Gen11 8SFF NC CTO Svr
Provedení, příslušenství	• Rackové provedení, max 2U

CPU	Min. 1x procesor o výkonu minimálně 24800 bodů dle http://cpubenchmark.net/, min počet jader 8																																																																														
RAM + HDD	- minimálně 256 GB RAM v provedení min. DDR5, min. 4800 MHz - Server musí disponovat alespoň 8x diskovou hotswap šachtou pro disky přístupnou zředu. Požadujeme osazení: - min. 3x NVMe SSD 7,68TB RI Hot Plug disky - bootovací zařízení 2x 480GB Raid 1																																																																														
Řadič disků:	- Řadič min. 4GB cache s ochranou proti výpadku napájení - podpora hot-plug disků SAS, SATA, NVMe - podpora min. RAID - 0, 1, 5, 6, 10, 50, 60																																																																														
Síťové karty:	4 x 10/25GbE SFP28 4x 1Gbit Base T																																																																														
Napájecí zdroje:	2x napájecí zdroj minimálně 1000W																																																																														
Management:	Plný vzdálený management umožňující plnou vzdálenou konzoli (html5), připojení lokálních médií																																																																														
Ostatní:	- Zásuvné ližiny pro rack - Podpora systémů: - Microsoft Windows Server - Red Hat® Enterprise Linux - SUSE Linux Enterprise Server																																																																														
Záruka, servis	Záruka na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru.																																																																														
Kompatibilita	Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu																																																																														
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	<table><tr><td>1</td><td>P52534-B21</td><td>HPE DL380 Gen11 8SFF NC CTO Svr</td></tr><tr><td>1</td><td>P52534-B21</td><td>HPE DL380 Gen11 8SFF NC CTO Svr</td></tr><tr><td>1</td><td>P49597-B21</td><td>INT Xeon-G 5415+ CPU for HPE</td></tr><tr><td>8</td><td>P43328-B21</td><td>HPE 32GB 2Rx8 PC5-4800B-R Smart Kit</td></tr><tr><td>1</td><td>P48813-B21</td><td>HPE DL380 Gen11 2U 8SFF x1 TM Kit</td></tr><tr><td>3</td><td>P64848-B21</td><td>HPE 7.68T NVMeRI SFF BC U.3ST V2 MV SSD</td></tr><tr><td>1</td><td>P26264-B21</td><td>BCM 57504 10/25GbE 4p SFP28 Adptr</td></tr><tr><td>1</td><td>P01366-B21</td><td>HPE 96W Smart Stg Li-ion Batt 145mm Kit</td></tr><tr><td>1</td><td>P48918-B21</td><td>HPE DL360 Gen11 Stg Cntrl Enable Cbl Kit</td></tr><tr><td>1</td><td>P58335-B21</td><td>HPE MR408i-o Gen11 SPDM Storage Cntrl</td></tr><tr><td>1</td><td>P51181-B21</td><td>BCM 5719 1Gb 4p BASE-T OCP Adptr</td></tr><tr><td>2</td><td>P03178-B21</td><td>HPE 1000W FS Ti Ht Plg PS Kit</td></tr><tr><td>1</td><td>BD505A</td><td>HPE iLO Adv 1-svr Lic 3yr Support</td></tr><tr><td>1</td><td>S1A05A</td><td>HPE Cmp Cloud Mgmt Srv FIO Enablement</td></tr><tr><td>1</td><td>P51911-B21</td><td>HPE DL360 Gen11 CPU1/OC2 x8 Enable Kit</td></tr><tr><td>1</td><td>P48820-B21</td><td>HPE DL380/DL560 G11 2U High Perf Fan Kit</td></tr><tr><td>1</td><td>P50400-B21</td><td>HPE DL3XX Gen11 2U Com Bezel Kit</td></tr><tr><td>1</td><td>P48183-B21</td><td>HPE NS204i-u Gen11 Ht Plg Boot Opt Dev</td></tr><tr><td>1</td><td>P49145-B21</td><td>HPE DL380 Gen11 Std Heat Sink Kit</td></tr><tr><td>1</td><td>P52152-B21</td><td>HPE DL380 G11 NS204i-u Internal Cbl Kit</td></tr><tr><td>1</td><td>P52341-B21</td><td>HPE DL3XX Gen11 Easy Install Rail 3 Kit</td></tr><tr><td>1</td><td>P54542-B21</td><td>HPE DL380 Gen11 NS204i-u FIO Kit</td></tr><tr><td>1</td><td>R7A12AAE</td><td>HPE COM Std 5yr Up ProLiant SaaS</td></tr><tr><td>1</td><td>HU4B2A5</td><td>HPE 5Y Tech Care Basic SVC</td></tr><tr><td>1</td><td>HU4B2A5</td><td>HPE iLO Advanced Non Blade Support</td></tr><tr><td>1</td><td>HU4B2A500DK</td><td>HPE DL380 Gen11 Support</td></tr></table>	1	P52534-B21	HPE DL380 Gen11 8SFF NC CTO Svr	1	P52534-B21	HPE DL380 Gen11 8SFF NC CTO Svr	1	P49597-B21	INT Xeon-G 5415+ CPU for HPE	8	P43328-B21	HPE 32GB 2Rx8 PC5-4800B-R Smart Kit	1	P48813-B21	HPE DL380 Gen11 2U 8SFF x1 TM Kit	3	P64848-B21	HPE 7.68T NVMeRI SFF BC U.3ST V2 MV SSD	1	P26264-B21	BCM 57504 10/25GbE 4p SFP28 Adptr	1	P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit	1	P48918-B21	HPE DL360 Gen11 Stg Cntrl Enable Cbl Kit	1	P58335-B21	HPE MR408i-o Gen11 SPDM Storage Cntrl	1	P51181-B21	BCM 5719 1Gb 4p BASE-T OCP Adptr	2	P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit	1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support	1	S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement	1	P51911-B21	HPE DL360 Gen11 CPU1/OC2 x8 Enable Kit	1	P48820-B21	HPE DL380/DL560 G11 2U High Perf Fan Kit	1	P50400-B21	HPE DL3XX Gen11 2U Com Bezel Kit	1	P48183-B21	HPE NS204i-u Gen11 Ht Plg Boot Opt Dev	1	P49145-B21	HPE DL380 Gen11 Std Heat Sink Kit	1	P52152-B21	HPE DL380 G11 NS204i-u Internal Cbl Kit	1	P52341-B21	HPE DL3XX Gen11 Easy Install Rail 3 Kit	1	P54542-B21	HPE DL380 Gen11 NS204i-u FIO Kit	1	R7A12AAE	HPE COM Std 5yr Up ProLiant SaaS	1	HU4B2A5	HPE 5Y Tech Care Basic SVC	1	HU4B2A5	HPE iLO Advanced Non Blade Support	1	HU4B2A500DK	HPE DL380 Gen11 Support
1	P52534-B21	HPE DL380 Gen11 8SFF NC CTO Svr																																																																													
1	P52534-B21	HPE DL380 Gen11 8SFF NC CTO Svr																																																																													
1	P49597-B21	INT Xeon-G 5415+ CPU for HPE																																																																													
8	P43328-B21	HPE 32GB 2Rx8 PC5-4800B-R Smart Kit																																																																													
1	P48813-B21	HPE DL380 Gen11 2U 8SFF x1 TM Kit																																																																													
3	P64848-B21	HPE 7.68T NVMeRI SFF BC U.3ST V2 MV SSD																																																																													
1	P26264-B21	BCM 57504 10/25GbE 4p SFP28 Adptr																																																																													
1	P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit																																																																													
1	P48918-B21	HPE DL360 Gen11 Stg Cntrl Enable Cbl Kit																																																																													
1	P58335-B21	HPE MR408i-o Gen11 SPDM Storage Cntrl																																																																													
1	P51181-B21	BCM 5719 1Gb 4p BASE-T OCP Adptr																																																																													
2	P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit																																																																													
1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support																																																																													
1	S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement																																																																													
1	P51911-B21	HPE DL360 Gen11 CPU1/OC2 x8 Enable Kit																																																																													
1	P48820-B21	HPE DL380/DL560 G11 2U High Perf Fan Kit																																																																													
1	P50400-B21	HPE DL3XX Gen11 2U Com Bezel Kit																																																																													
1	P48183-B21	HPE NS204i-u Gen11 Ht Plg Boot Opt Dev																																																																													
1	P49145-B21	HPE DL380 Gen11 Std Heat Sink Kit																																																																													
1	P52152-B21	HPE DL380 G11 NS204i-u Internal Cbl Kit																																																																													
1	P52341-B21	HPE DL3XX Gen11 Easy Install Rail 3 Kit																																																																													
1	P54542-B21	HPE DL380 Gen11 NS204i-u FIO Kit																																																																													
1	R7A12AAE	HPE COM Std 5yr Up ProLiant SaaS																																																																													
1	HU4B2A5	HPE 5Y Tech Care Basic SVC																																																																													
1	HU4B2A5	HPE iLO Advanced Non Blade Support																																																																													
1	HU4B2A500DK	HPE DL380 Gen11 Support																																																																													



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Parametr	Minimální požadavek
Výrobce a model	2x HPE MS WS25 16C DC OEM CZ/ ENG 85x HPE MS WS25 Dev CAL licence 5x HPE MS WS25 Ushr CAL licence
Parametry	2 ks licencí 64-bitového serverového operačního systému v aktuální verzi • Podpora min. 64 procesorových socketů • Podpora běhu v on-premise, hybrid a cloudovém prostředí • Podpora TPM 2.0 čipů • Podpora ochrany firmware před neoprávněným přepsáním • Podpora replikace úložišť • Vestavěná technologie serverové i desktopové virtualizace • Nativní podpora virtualizace sítí • Neomezený počet virtuálních serverů • Počet licencí bude určen počtem jader procesorů ve všech navržených serverech – min 2x16CORE • Operační systém musí být kompatibilní s již provozovanými aplikacemi. Aktuálně zadavatel provozuje operační systémy od společnosti MICROSOFT. • licence pro nabízené operační systémy umožňující využívat těchto systémů minimálně pro 85 zařízení + 5 uživatelů
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	

Software Defined Storage

Parametr	Minimální požadavek
Výrobce a model	2x StarWind Virtual SAN Unlimited Edition for 1 node, 5year of Standard ASM
Parametry	• Nabízené řešení Software Defined Storage (SDS) bude využívat SAN infrastrukturu na protokolu iSCSI. • SDS musí umět virtualizovat kapacitu z vnitřních úložišť a tuto kapacitu poskytovat pomocí standardního protokolu. • Kromě SDS musí být v nodech storage clusteru provozovatelné také virtuální servery. • Nabízené řešení musí být široce škálovatelné • SDS musí podporovat min. OS Windows 2008 R2, a vyšší, Linux, VMware 6.0 a vyšší, Hyper-V, včetně „multi-path“ připojení • Podpora autentizace uživatelů přes Active Directory • Řešení musí podporovat SSD, SAS i NL-SAS disky v jednom nodu současně. • SDS musí umět vytvořit logický disk (LUN) o velikosti min.64TB • Čistá kapacita storage clusteru musí být nelimitovaná • Řadiče diskového pole musí podporovat režim active/active a automaticky rozkládat zátěž každého LUNu na všechny disky v dané vrstvě. • Nabízené řešení musí využívat min. 10 Gbit technologii • Storage musí podporovat No Single Point of Failure řešení tak, aby při havárii libovolného storage nodu/řadiče provoz plynule pokračoval bez odstávky. Rovněž upgrade systému storage clusteru (HV, firmware ...) musí být možné provést bez přerušení provozu. • Řešení umožní synchronní replikaci dat mezi uzly clusteru pro zvolené datové oblasti na úrovni nodů clusteru a synchronní replikaci LUNů mezi dvěma lokalitami. • Podpora protokolu NVMe-oF minimálně na platformě Hyper-V • Řešení musí podporovat min.tyto protokoly: iSCSI, SMB 3.0, NFS V4 • Podpora VVols pro VMware prostředí • Podpora Write-Back Cache pro ukládání dat do mezipaměti, která je uzpůsobená pro intenzivní virtualizovaná pracovní vytížení. • Požadujeme licence pro následující funkce:



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	- kompletní management/GUI a command line. Grafické rozhraní pro správu musí být intuitivní a jednoduše ovladatelné. - snapshot – až 64 snapshotů z jednoho logického disku - thin provisioning - synchronní replikace mezi NODy - podpora multipathing a Microsoft MPIO DSM - Podpora VMware VAAI - Řešení musí umožňovat detailní reporting o okamžité i historické vytiženosti SDS - Podpora produktu poskytovaná výrobcem na dobu 5 let (v ceně licence)
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	

2) nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA – 2 core a 1 přístupový SWITCH

Parametr	Minimální požadavek
Výrobce a model	2x Catalyst C1300-12XS PN C1300-12XS 2x 19-in. rack-mount bracket for C1000, C1200, C1300, 1x Catalyst C1300-48T-4X PN C1300-48T-4X 2x Cisco SFP-H10GB-CU1M= 10GBASE-CU SFP+ Cable 1 Meter 10x Cisco SFP-H10GB-CU3M= 10GBASE-CU SFP+ Cable 3 Meter 6x Cisco SFP-H10GB-CU5M= 10GBASE-CU SFP+ Cable 5 Meter 30x 10G SFP+ Transceiver SM
Základní vlastnosti	- Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení - Podpora výrobce pro řešení technických problémů platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení. - IEEE 802.3ad (Link Aggregation) - IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis - Minimálně 8 linek jako součást Link Aggregation Group trunku - Minimální počet konfigurovatelných Link Aggregation Group trunků: 16 - IEEE 802.1Q - Minimální počet aktivních VLAN: 4093 - IEEE 802.1x - Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) - Podpora instance spanning-tree protokolu per VLAN - IEEE 802.1w - Rapid Spanning Tree Protocol - Protokol MVRP/GVRP nebo VTP pro definici a správu VLAN sítí - Podpora jumbo rámců (min. 9000 bytes) - Detekce protilehlého zařízení (např. CDP nebo LLDP) - Směrování protokolů IPv4 a IPv6 v hardware - IGMPv2, IGMPv3 - IGMP snooping - MLD snooping - Minimální počet HW QoS front: 8 - QoS classification – ACL, DSCP, CoS based - IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) - Možnost definovat povolené MAC adresy na portu - Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	- Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru - Bezpečnostní funkce umožňující inspekci provozu protokolu ARP - HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů - IEEE 802.3az. - Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu. - SSHv2. - CLI rozhraní. - SNMPv2/v3. - TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting). - Záruka dohledatelná na webových stránkách výrobce, stahování aktualizací a řešení servisních případů přímo na webových stránkách výrobce zařízení
Technické požadavky na agregační přepínač LAN - 2ks	- L2/L3 přepínač - Rackmount provedení pro 19" rozvaděč - Stohovatelný switch, minimálně 8 zařízení v jednom stohu - Rozměr 1 RU 10x 10GE SFP+ porty 2x combo 10G SFP+/ 10GbitBase-T 1x RJ45 1Gbit Management port - Minimální kapacita přepínání 240 Gbps - Minimální paketový výkon přepínače 178 Mpps - minimálně 4093 aktivních VLAN - Minimální počet záznamů MAC tabulky 16 000 - Minimální počet MST Spanning tree instancí 8 - Minimální počet záznamů v routovací tabulce 900 (pro IPv4) - Packet buffer minimálně 1,5MB
Technické požadavky na přístupový přepínač LAN - 1ks	- L2/L3 přepínač - Rackmount provedení pro 19" rozvaděč - Stohovatelný switch, minimálně 8 zařízení v jednom stohu - Rozměr 1 RU 48x 10/100/1000Mbit RJ45 porty 4x 10G SFP+ porty - Minimální kapacita přepínání 176 Gbps - Minimální paketový výkon přepínače 130 Mpps - minimálně 4093 aktivních VLAN - Minimální počet záznamů MAC tabulky 16 000 - Minimální počet MST Spanning tree instancí 8 - Minimální počet záznamů v routovací tabulce 900 (pro IPv4) - Packet buffer minimálně 1,5MB
Spojovací materiál	30x 10G SFP+ Transceiver SM 2x DAC kabel 10Gbit, 1M 10x DAC kabel 10Gbit, 3M 6x DAC kabel 10Gbit, 5M - Optické moduly a DAC kabely musí podléhat stejné záruce jako switche - Další drobný a propojovací materiál nutný k plnohodnotné realizaci díla jednotlivě nespecifikovaný (optické propojovací kabely, metalické propojovací kabely, napájecí kabely atd)
Certifikace dodavatele, původ zboží	Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

3 - Systém pro analýzu síťového provozu a bezpečnostní monitoring

TECHNICKÁ SPECIFIKACE :

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Nabízená technologie musí být určená pro provoz v ČR. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, ...“ je uvedený parametr závazný a požadovaná funkcionality musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, dodavatel může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nespĺňuje, vč. vysvětlení, jak je zadání splněno
Systém pro analýzu síťového provozu	
Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.	Splňuje, všechny požadavky splňuje produkt: GREYCORTEX Mendel perpetuální SW licence: senzor + kolektor / 100Mbps trvalý průtok / 120 obohacených toků za vteřinu & 250 NetFlow za vteřinu / HW server All-in-one model XS / 2x1GbE monitorovací rozhraní / 800GB SSD RAID1 datové úložiště / 5 roků DELL HW On-Site NBD support, pětiletá SW podpora a údržba pro MA-SC-100-SW
Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	Splňuje
Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	Splňuje
Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	Splňuje
Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	Splňuje
Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	Splňuje

Zpracování a ukládání síťových toků	
Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	Splňuje
Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.	Splňuje
Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 3 měsíců složené z SSD nebo NVMe disků.	Splňuje
Analýza aplikačních a systémových logů Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.	Splňuje
Uživatelské rozhraní	
Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	Splňuje
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	Splňuje
granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),	Splňuje
granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),	Splňuje
vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	Splňuje
vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	Splňuje
Automatické hlášení (alerty) a reporting	
Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	Splňuje
Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro využití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	Splňuje
Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniku (např.: doména, web, email apod.).	Splňuje

Je požadováno vytváření automatizovaných reportů v českém jazyce.	Splňuje
Integrace systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	Splňuje
syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	Splňuje
přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	Splňuje
export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP	Splňuje
integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Microsoft Active Directory	Splňuje
integrace s firewall řešením pro automatické a manuální reakce vyvolané systémem	Splňuje
integrace s nástroji pro řízení přístupu k síti pro automatickou a manuální reakci systému.	Splňuje

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nespĺňuje, vč. vysvětlení, jak je zadání splněno
Obecné požadavky pro nasazení	
Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19".	Splňuje
Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	Splňuje
Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.	Splňuje
Požadavky pro pokrytí IT prostředí	
Je požadován 1x HW datový kolektor/senzor o celkové propustnosti minimálně 100Mbps pro 200 monitorovaných IP adres s monitorovacím rozhraním 2x1GbE.	Splňuje

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nespĺňuje, vč. vysvětlení, jak je zadání splněno
Monitorování zařízení, segmentů sítě a využívaných síťových služeb	
Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	Splňuje
změna IP/MAC adresy hosta,	Splňuje

• duplicitní IP/MAC adresa,	Splňuje
• změna VLAN,	Splňuje
• vytvoření nové podsítě,	Splňuje
• připojení nového zařízení,	Splňuje
• použití nebo vznik nové služby,	Splňuje
• nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	Splňuje
• přístup nového zařízení ke službě či zařízení	Splňuje
• ověřování platnosti interních certifikátů pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	Splňuje
Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.	Splňuje
Samostatné učení behaviorálních aktivit a detekce anomálií	
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	Splňuje
Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	Splňuje
• odchylku od modelu pro přenos dat, toků a paketů,	Splňuje
• odchylku od modelu pro počet komunikačních partnerů,	Splňuje
• odchylku od modelu entropie na komunikačních portech,	Splňuje
• odchylku od modelu pro počet síťových toků a využitých síťových služeb,	Splňuje
• odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	Splňuje
Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	Splňuje
Identifikace neznámých hrozeb a podezřelých chování	
Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	Splňuje
• průzkumné aktivity v síti,	Splňuje
• detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	Splňuje



**Národní
plán
obnovy**



**Financováno
Evropskou unií
NextGenerationEU**



**MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY**

• detekce repetitivních vzorců chování na síti,	Splňuje
• detekce botnetů a ovládání kompromitované stanice,	Splňuje
• detekce příznaků těžení kryptoměn,	Splňuje
• útoky hrubou silou a enumerace dat,	Splňuje
• rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	Splňuje
Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě	Splňuje
• detekční databáze známých hrozeb, tj. malware (trojské koně, víry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,	Splňuje
• reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	Splňuje
Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	Splňuje
Uživatel musí být schopen importovat vlastní záznamy.	Splňuje
Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	Splňuje
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	Splňuje
Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. Příklad možné syntaxe detekčního pravidla: <code>alert tcp \$HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";)</code>	Splňuje
Analýza šifrované komunikace Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.	Splňuje
Asistované učení	
Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	Splňuje
• IP adresa,	Splňuje

• MAC adresa,	Splňuje
• hostname,	Splňuje
• segment sítě / podsítě,	Splňuje
• lokalita – ASN, země apod.	Splňuje
• směr komunikace – určení klienta, nebo serveru,	Splňuje
• detekovaná událost – kategorie, název apod.	Splňuje
• použité služby, protokolu, portu,	Splňuje
• libovolné kombinaci výše popsaných.	Splňuje
Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	Splňuje

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nespĺňuje, vč. vysvětlení, jak je zadání splněno
Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	Splňuje
Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	Splňuje
• podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	Splňuje
• prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	Splňuje
Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	Splňuje
Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	Splňuje
Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http	Splňuje

hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.	
Systém umožňuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	Splňuje
Kontextuální informace	
Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	Splňuje
jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie	Splňuje
hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu	Splňuje
IP geolokace	Splňuje
IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	Splňuje
historie použitých MAC adresa a výrobce zařízení	Splňuje
operační systém a jeho historie na zařízení	Splňuje
uživatelé zadané poznámky a informace k zařízení	Splňuje
automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	Splňuje
seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.	Splňuje
seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	Splňuje
Zaznamenávání, ukládání a zpětná analýza plného provozu	
Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsít, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	Splňuje
Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru.	Splňuje
Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.	Splňuje
Další požadované oblasti využití	
Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nespĺňuje, vč. vysvětlení, jak je zadání splněno

Monitorování politik kybernetické bezpečnosti	
Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	Splňuje
monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	Splňuje
detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	Splňuje
Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomoci:	Splňuje
uživatelé definované podsítě na základě rozsahů IP adres	Splňuje
uživatelsky libovolně definovaných skupin zařízení	Splňuje
automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	Splňuje
Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	Splňuje
spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,	Splňuje
jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	Splňuje
možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.),	Splňuje
možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	Splňuje
možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	Splňuje
Detekce úniku dat	
Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	Splňuje
Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	Splňuje
V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	Splňuje
název souboru,	Splňuje
velikost souboru,	Splňuje



**Národní
plán
obnovy**



**Financováno
Evropskou unií
NextGenerationEU**



**MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY**

HASH souboru.	Splňuje
Monitoring výkonu aplikací a sítě	
Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	Splňuje
přenosová rychlost sítě,	Splňuje
rychlost odezvy aplikace,	Splňuje
odezva systému z pohledu uživatele.	Splňuje
Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	Splňuje
všechny porty a služby TCP,	Splňuje
pro všechny kombinace služeb a zařízení.	Splňuje
Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewallly.	Splňuje
Monitoring cloudových služeb	
Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.	Splňuje
Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.	Splňuje
Inventarizace sítě a grafická vizualizace topologie	
Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	Splňuje
Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.	Splňuje
Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.	Splňuje
Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.	Splňuje

Implementační služby

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekovány nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

Produktová podpora výrobce

Dodavatel musí zajistit:

- softwarovou produktovou podporu řešení v délce 60 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.
- záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

Administrátorské školení

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele.

Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

4 - NAS

Parametr	Minimální požadavek
Výrobce a model	1x Synology RS2423+ Rack Station 4x Synology HAT5300/ 16TB/ HDD/ 3.5"/ SATA/ 7200 RPM/ 5R 1x Sada ližin Synology, RKS-02 1x Synology Kombinovaný adaptér M.2 SSD a 10GbE E10M20-T1 2x Synology SNV3510/800GB/SSD/M.2 NVMe/5R 1x Synology NBD HW rpl RS2423+
Parametry	• NAS, rackmount provedení včetně lyžin • Čtyřjádrový procesor v architektuře x86 64 bit • Systémová paměť 8 GB DDR4 2666 MHz, rozšiřitelná do 32GB • Pozice pro diskové jednotky ◦ 12 x 3,5" nebo 2,5" SATA HDD/SSD • Kompatibilita diskových jednotek ◦ 3,5" SATA jednotky pevných disků ◦ 2,5" SATA SSD • Diskové jednotky vyměnitelné za provozu • Min.2x Gigabitový Ethernet port (RJ45) • 2x 10GbE Base-T (RJ45) • 2x pozice pro M.2 SSD NVMe, Podporovaný rozměr: 22110 / 2280 • 2x disk SSD M.2 800GB, TWB 1022TB, stejný výrobce jako NAS • USB port ◦ 2x USB 3.0 • Disky: ◦ 4x16T HDD stejný výrobce jako NAS a určen pro provoz v NAS ◦ rozhraní SATA III (6 Gb/s), ◦ rychlost 7 200 ot./min. • Záruka 5LET NBD
Další informace či odkazy dodavatele k nabízenému plnění	



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

(nepovinné
pole)

5) nástroj pro ochranu koncových stanic

Ochrana koncových stanic a SVR

Specifikace pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR.

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux s možností rozšíření ochrany pro mobilních zařízení. Požadovaný počet licencí je 150.

Základní požadavky na řešení

Řešení pro komplexní ochranu PC, Linux, Mac, fyzické a virtuální serverové infrastruktury musí být spravováno z jedné webové konzole. Výrobce nesměl získat na av-comparatives (<https://www.av-comparatives.org/awards/>) za poslední 2 roky ani jednou méně než 3 hvězdy v kategorii „Real World Protection“ u firemních řešení.

Detailní požadavky na správu a funkcionalitu naleznete podle kategorií a funkcí níže.

Následující funkce jsou bezvýhradně nutné k splnění podmínek výběrového řízení:

1. Konzole pro centrální správu řešení:

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů	ANO	Uvedené požadavky splňuje Bitdefender GravityZone Business Security Enterprise (Ultra) - 60 M – GOV (150 licencí)
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí	ANO	
Možnost kdykoli zmigrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení	ANO	
Konzole pro centrální správu je kompletně multi-tenantní	ANO	
Základní vlastnosti		
Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu	ANO	
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem	ANO	
Možnost zasílat upozornění napojením na Syslog server	ANO	

Možnost využití napojení jakékoli třetí aplikace za pomoci zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce	ANO	
Úlohy správy bezpečnosti		
Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.	ANO	
Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery	ANO	
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	
Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy	ANO	
Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy	ANO	
Centralizované místo pro záznam všech úloh	ANO	
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulórně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)	ANO	
Nastavení úrovně bezpečnosti		
Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD	ANO	
Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulórně dle sekcí a subsekcí nastavení bezpečnostních pravidel	ANO	
Reportování		
Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě	ANO	
Možnost zasílání vygenerovaných reportů e-mailem	ANO	
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	
Karanténa		

Vzdálená obnova či smazání souboru v karanténě	ANO	
Možnost automaticky přidat soubor do výjimky při obnově z karantény	ANO	
Uživatelé		
Více předdefinovaných rolí: Root, administrátor, reportér 1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty	ANO	
Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)	ANO	
Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny	ANO	
Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení	ANO	
Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat	ANO	
Logy		
Zaznamenávání uživatelských akcí	ANO	
Detailní log pro každou akci	ANO	
Komplexní vyhledávání v logách	ANO	
Správa a instalace ochrany		
Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány	ANO	
Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 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	
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 správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích	ANO	

Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů	ANO	
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou	ANO	
Pro rozdílné skupiny uživatelů lze granulórně nastavit, jaké skupiny zařízení mají právo spravovat	ANO	
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti	ANO	
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)	ANO	
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	

2. Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Podpora operačních systémů: Windows 10 1507 a vyšší Windows 8.1 Windows 8 Windows 7 Windows 10 IoT Enterprise Windows Embedded 8.1 Industry Windows Embedded 8 Standard Windows Embedded Standard 7 Windows Embedded Compact 7 Windows Embedded POSReady 7 Windows Embedded Enterprise 7 Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Windows Server 2012 Windows Small Business Server 2011 Windows Server 2008 R2 Ubuntu 14.04 LTS a vyšší Red Hat Enterprise Linux CentOS 6.0 a vyšší	ANO	

SUSE Linux Enterprise Server 11 SP4 a vyšší OpenSUSELeap 42.x Fedora 25 a vyšší Debian 8.0 a vyšší Oracle Linux 6.3 a vyšší Amazon Linux AMI 2016.09 a vyšší Mac OS X El Capitan (10.11) a vyšší		
Automatické skenování dat, ke kterým je přístupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů	ANO	
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru	ANO	
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu	ANO	
Detekce na základě virových definicí (tzn. signatur)	ANO	
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykazování 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	
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)	ANO	
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně	ANO	

Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno	ANO	
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky	ANO	
Možnost automatické detonace podezřelých souborů v Sandboxu	ANO	
Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne	ANO	
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu	ANO	
Možnost ručního vložení vzorku do Sandboxu	ANO	
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímků obrazovky případných chybových hlášení	ANO	
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP	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 umožňuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.	ANO	
Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem	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 ukládat data o bezpečnostních incidentech až 90 dní	ANO	
Možnost prověřovat http provoz	ANO	
Možnost prověřovat provoz šifrovaný pomocí SSL	ANO	
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic	ANO	

Automatické skenování emailů na úrovni pracovní stanice, neohledě na použitý emailový klient, obojí pro odchozí (SMTP) a příchozí emaily (POP3)	ANO	
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů	ANO	
Ochrana proti podvodným a phishingovým webovým stránkám	ANO	
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID	ANO	
Možnost rozšíření o správu patchů aplikací třetích stran	ANO	
Možnost rozšíření o správu šifrování pevných disků	ANO	
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)	ANO	
Firewall		
Možnost blokovat skenování portů	ANO	
Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS	ANO	
Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb	ANO	
Možnost vypnout IDS	ANO	
Možnost nastavit profily známých sítí	ANO	
Možnost blokování Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu	ANO	
Karanténa		
Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě	ANO	
Možnost obnovy souboru do originální či do nově zadané lokality	ANO	
Automatické mazání souborů v karanténě starších než zadaná maximální doba stárí (maximum nesmí být kratší než 30 dní)	ANO	
Kontrola přístupu k internetu		
- Zablokování přístupu na internet pro specifické stanice / skupiny stanic - Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic - Zablokování přístupu k internetu v určený čas - Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) - Zamezení přístupu ke konkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)	ANO	

3. Ochrana virtualizovaných koncových bodů (Windows, Linux)

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen	ANO	
„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením	ANO	
„Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže	ANO	
Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení	ANO	
Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)	ANO	
Automatické skenování dat, ke kterým je přístupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů	ANO	
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru	ANO	
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu	ANO	
Detekce na základě virových definicí (tzn. signatur)	ANO	
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykazování 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	



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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	
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)	ANO	
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně	ANO	
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno	ANO	
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky	ANO	
Možnost automatické detonace podezřelých souborů v Sandboxu	ANO	
Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne	ANO	
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu	ANO	
Možnost ručního vložení vzorku do Sandboxu	ANO	
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímků obrazovky případných chybových hlášení	ANO	
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP	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 umožňuje 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 zachycení incidentu za účelem dalšího prověřování	ANO	
Možnost prověřovat http provoz	ANO	
Možnost prověřovat provoz šifrovaný pomocí SSL	ANO	
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic	ANO	
Automatické skenování emailů na úrovni pracovní stanice, neohledně na použitím emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)	ANO	
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů	ANO	
Ochrana proti podvodným a phishingovým webovým stránkám	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	
Podpora 60 měsíců	ANO	
Akceptační podmínky: • Veškeré komponenty systému jsou řádně licencované • Bylo dodáno zařízení dle požadované technické specifikace • Všechny komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele. • Byla vytvořena a dodána provozní dokumentace. • Bylo provedeno školení v požadovaném rozsahu	ANO	
Produkty, které dodavatel dodává v rámci plnění zadavatel, musí splňovat následující podmínky • jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce, • 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 a určeny pro tento konkrétní projekt • jsou určeny pro provoz v České republice. • Tyto skutečnosti dodavatel doloží potvrzením výrobce nebo oficiálního distributora tohoto zařízení	ANO	

6) nástroj pro ověřování identity uživatelů



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Parametr	Minimální požadavek
Výrobce a model	FortiTokenMobile (Electronic License), FortiTokenMobile FTM-ELIC-100
Parametry	• Trvalá licence pro mobilní platformy (Android, IOS) • Podpora stávajícího firewallu FortiGate 60F • Plná integrace s uvedeným Firewalem • Licence použitelná pro realizaci 2FA pro přihlášení minimálně na VPN • Podpora time-based i event-based autentifikačních tokenů • Push notifikace • Licence pro 100 koncových uživatelů
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	

7) nástroj pro ochranu a zabezpečení e-mailů

Parametr	Minimální požadavek
Výrobce a model	FortiMail-VM01, SW virtual appliance FortiMail-VM01, Licence, 24x7 Base Bundle Contract 5YR
Parametry	• Řešení na ochranu emailové komunikace (bezpečná emailová brána) fungující jako VM appliance (proprietární operační systém výrobce včetně všech funkcí) v prostředí Vmware/HyperV/KVM. Řešení HW appliance, anebo jako software není přípustné. Součástí musí být podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let • Podpora až 4 síťových rozhraní v rámci síťového prostředí hypervisoru • VM appliance alokuje min. 1 vCPU • VM appliance alokuje min. 4 GB paměti • VM appliance alokuje min. 2 TB diskového prostoru • Možnost nasazení v režimu MTA gateway nebo transparentní režim • Možnost nasazení v režimu vysoké dostupnosti (včetně sdílení fronty) pro budoucí rozšíření • Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky (NG Firewall, sandbox) za účelem sdílení telemetrických informací a informací o odhalených hrozbách (škodlivém kódu) sandboxovací technikou. • Ochrana proti škodlivému kódu, nevyžádané elektronické pošty a uniku citlivých dat • Podpora víceúrovňové detekce nevyžádané pošty (IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza) • reakce na detekovaný spam minimálně: přidání tagu, přidání hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce • Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky) • Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	škodlivého kódu, odstranění aktivního obsahu PDF a kancelářských dokumentů, karanténa, odstranění škodlivých odkazů z emailů, AV kontrola musí být plně integrována s platformou Sandbox (viz níže), umožňující pokročilou ochranu před pokročilými typy hrozeb včetně tzv. zero-day útoků. Na rozdíl od firewallu tato integrace musí být v režimu pozdržení emailu ve frontě až do konce analýzy na sandboxu, sdílení signatur dynamicky vytvářených na platformě sandbox • Podpora IPv6 • Podpora VLAN • Plnohodnotná integrace s LOG serverem a SIEM platformou. • Plnohodnotná integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem). • Výkonové požadavky • Propustnost min. 50 000 emailů za hodinu při průměrné velikosti email ~100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu • Podpora ochrany minimálně 100 emailových domén • Licenčně nezávislý model na počtu uživatelů, mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek) • Certifikace VB verified spam + • Certifikace VB 100 Virus • Certifikace ICASA labs • Certifikace AAA SE Labs
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	

8 - Dodávka a implementace nástroje pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

Parametr	Minimální požadavek	
Výrobce a model	LOGM-M-5Y Logmanager M, 1U server, 5 let HW a SW support, 4x4TB disky	Splňuje Ano/Ne



Základní vlastnosti	• Navrhnout, dodat a implementovat nástroj na zaznamenávání událostí. Tento nástroj bude sloužit pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele určeným hodnocením aktiv a bezpečnostních potřeb organizace. Navržený nástroj musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, vyplývajících zejména z připravované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšší povinnosti (NIS2). Nástroj proto musí být schopen zaznamenat všechny bezpečnostní a relevantní provozní události a tyto uchovat nejméně po dobu 18 měsíců. Nástroj musí být dále schopen zajistit přesné časové razítko ke všem pořízeným událostem a umožnit zachování důvěrnosti a integrity pořízených dat po celou dobu jejich životního cyklu. Pro efektivní využití musí nástroj umět generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem. • Cílem je mít jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Nástroj musí dále umožňovat snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalosti programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů. • Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný nástroj podporoval možnost horizontálního i vertikálního rozšíření formou clusteru a dále plánované i ad-hoc zálohování vzniklých dat na externí zálohovací systém. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců. Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametry uložených dat. • Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Ne všichni naši administrátoři a budoucí operátoři systému dokonale ovládají angličtinu, proto požadujeme, aby součástí dodávky byla i dokumentace v českém jazyce, obsahem i kvalitou srovnatelná s aktuální dokumentací v angličtině. Proto v rámci odpovědi na výběrové řízení požadujeme předložit kompletní dokumentaci k celému systému a poznámky k vydání (release notes) k systému i všem návazným komponentům. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Dodaný systém plánujeme provozovat vlastními lidskými zdroji, proto by nabízený systém měl umožňovat našim pracovníkům IT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený nástroj proto musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používání skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem. • Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory. • V případě pochybností o vlastnostech nabízeného nástroje si vyhraujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek s technickými parametry nabízeného řešení do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále	
----------------------------	--	--



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	si vyhrazujeme právo vyžádat kontakty alespoň na 3 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.	
Technická specifikace	Zadavatel vyžaduje, aby nabízené řešení mělo níže požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.	Ano
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Splňuje
1	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.	Ano
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	Ano
3	Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	Ano
4	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	Ano
5	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

6	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.	Ano
7	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	Ano
8	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	Ano
9	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.	Ano
10	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano
11	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	Ano
12	Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	Ano
13	Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.	Ano
14	Systém provádí konsolidaci logů na interním storage logovacího systému.	Ano
15	Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.	Ano
16	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.	Ano

17	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohlédávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohlédávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	Ano
18	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohlédávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohlédávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	Ano
19	Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Microsoft365.	Ano
20	V případě krátkodobého (do 10 minut) až dvouásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	Ano
21	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	Ano
22	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	Ano
23	Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	Ano
24	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano
25	Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	Ano
26	Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.	Ano
27	Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.	Ano
28	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB.	Ano
29	Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení.	Ano
30	Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

31	Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	Ano
32	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.	Ano
33	Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.	Ano
34	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	Ano
	Minimální HW parametry požadovaného systému	
38	Jedna hardwarová appliance o velikosti max. 1U, včetně lyžin umožňujících vysunutí zapnutého systému z racku pro servisní účely.	Ano
39	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	Ano
40	1 procesor, min. 16 jader, s podporou HyperThreadingu nebo Multi-Threadingu.	Ano
41	RAM Min. 64GB DDR-4.	Ano
42	Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	Ano
43	Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	Ano
44	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.	Ano
45	Ventilátory redundantní a vyměnitelné za provozu.	Ano
46	Napájecí zdroje redundantní a vyměnitelné za chodu (hotplug).	Ano
47	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače).	Ano
48	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	Ano
	Výkonnostní a SW parametry systému	
49	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

50	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	Ano
51	Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade, nebo přiložte odkaz na dokumentaci s detailním popisem.	Ano
52	Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	Ano
53	Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalém příjmu událostí.	Ano
54	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat.	Ano
55	Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	Ano
56	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.	Ano
57	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	Ano
58	V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...	Ano
59	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

60	Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení skriptů, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.	Ano
61	Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožňuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.	Ano
62	V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.	Ano
63	V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	Ano
64	Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	Ano
65	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	Ano
66	Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	Ano
	Alerty	
67	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	Ano
68	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	Ano
69	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	Ano
70	Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložení příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testování alertů a korelací.	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

71	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.	Ano
72	V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	Ano
73	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.	Ano
Sběr událostí z Microsoft prostředí		
74	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.	Ano
75	Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahod' logy s EventId 7036.	Ano
76	Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.	Ano
77	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.	Ano
78	Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.	Ano
79	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.	Ano



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

80	Počet instalací Windows agenta by neměl být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 200 na dobu předpokládané morální životnosti produktu – 7 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit zda systém výkonnostně splňuje tento požadavek. Jedná se o klíčovou funkci, proto budeme před uzavřením smlouvy požadovat předvedení požadovaných funkcí, stability i výkonnostní kapacity nabízeného systému pro sběr logů z prostředí Microsoft.	Ano
Podpora pro sběr událostí z poboček		
81	Systém musí podporovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.	Ano
82	Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	Ano
83	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášet data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	Ano
84	Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven přístup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení řešení pro sběr událostí na pobočkách.	Ano
85	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	Ano
86	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	Ano
87	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	Ano
88	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	Ano
89	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	Ano
Vysoká dostupnost, SW Podpora a záruka na hardware		
90	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.	Ano
91	HW - Požadovaná minimálně 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	Ano
92	Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	Ano
93	SW - Podpora výrobce na aktualizaci systému a parserů na 5 let . Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	Ano

Akceptační podmínky	• Veškeré komponenty systému jsou řádně licencované • Bylo dodáno fyzické zařízení dle požadované technické specifikace.
---------------------	---



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	- Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele. - Byla vytvořena a dodána provozní dokumentace. - Bylo provedeno školení v požadovaném rozsahu
--	---

9 Ochrana počítačové sítě před malwarem a zneužíváním zařízení na úrovni DNS překladač, řešení poskytujícího plnou kontrolu nad DNS provozem.

Parametr	Minimální požadavek
Výrobce a model	Whalebone Immunity User Business support 60 měsíců
Základní vlastnosti	- Produkt poskytuje ochranu na úrovni DNS proti: - Malware - Detekce Zero-day pomocí generátoru domén (DGA) - Homografické phishingové útoky - Komunikace C&C - Exploit, Backdoor, Trojan, Keyloggerům - Spamu - Škodlivému coinminingu - DNS tunnelingu - DNS cache poisoningu - DNS rebinding útokům - Detekce anomálií DNS a upozorňování na ně - Nevyžaduje modifikaci na koncových stanicích - Není třeba instalovat SW na koncové stanice - Bez nutnosti ruční rekonfigurace, vše musí být provedeno automaticky - Není třeba instalovat certifikáty ani resetovat bezpečnostní politiky
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků základních vlastností	Whalebone Immunity splňuje všechny požadované základní vlastnosti, instalace probíhá pouze instalací DNS serveru na linux virtuální servery, bez nutnosti úprav na koncových bodech, ty jsou automaticky a ihned chráněny.
Požadavky na administrační portál	- Webové rozhraní pro správce je plně přístupné prostřednictvím moderních webových prohlížečů bez nutnosti instalace doplňků nebo místního softwaru potřebného pro přístup k rozhraní. - Možnost aktivovat dvoufaktorovou autentizaci a vynutit ji pro všechny správce v organizaci - Možnost omezit přístup k rozhraní správce pouze z místní sítě nebo z definovaných veřejných IP rozsahů - Různá nastavení autorizace (pro jednotlivé skupiny) dostupná pro operátory v minimálně 2 rolích: - Administrátor - Uživatel s právy pouze pro čtení - K dispozici je log provozu DNS ze všech resolverů s možností fulltextového filtrování v rozhraní. - Podrobnosti o všech unikátních požadavcích/odpovědích budou přístupné a exportovatelné pro další analýzu ve formátu csv



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	• Webové rozhraní poskytuje přístup ke následujícím funkcím: ○ Analýza hrozeb ○ Analýza provozu DNS ○ Analýza content filteringu ○ Konfigurace nastavení filtrace a bezpečnostních politik: Konfigurace bezpečnostních politik ○ Konfigurace blokace regulatorních feedů ○ možnost vytváření vlastních whitelistů a blacklistů ○ Konfigurace white-label blokačních stránek ○ Konfigurace nastavení resolveru ○ Správa DNS resolveru: ○ Přehled resolverů ○ Přiřazení bezpečnostních politik konkrétním rozsahům IP adres ○ Možnosti upgradu / aktualizace verze resolveru ○ Možnosti pokročilé konfigurace ○ Procházení auditních logů o aktivitách uživatelů v portálu ○ Alerting
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na administrační portál	Whalebone Immunity disponuje admimistračním rozhraním, které splňuje veškeré požadované parametry.
Požadavky na další funkce a komponenty	• On-premise řešení: ○ Plně autonomní DNS resolver s bezpečnostní vrstvou, která provádí filtraci a překlad DNS bez nutnosti komunikace s externí službou v cloudu. ○ V souladu se standardy RFC ○ Bezpečnostní vrstva umožňuje přesměrování požadavků u nebezpečných domén na blokační stránku. ○ Vyžaduje DNSSEC validaci včetně negativního ukládání do mezipaměti NSEC3 ○ Změny konfigurace a aktualizace resolveru jsou prováděny za plného provozu - bez výpadku služby a bez výpadku provozu DNS, během aktualizací a rekonfigurací ○ Podpora DNS přes TLS (DoT) a DNS přes HTTPS (DoH) • Blokační stránka: ○ Webová stránka, na kterou je uživatel přesměrován, když se on nebo jeho zařízení pokusí o přístup k inkriminované webové stránce. ○ Blokační stránku lze libovolně upravit podle přání zákazníka tak, aby respektovala firemní identitu a vizuální stránku (písmo, barvy, logo, kontakty) ○ Funkce „ByPass“ pro definované sítě - uživatel může pokračovat na cílovou doménu, aniž by vyžadoval spolupráci správce (např. pro sítě hostů). Správa provozu DNS a brány firewall: ○ Konkrétní zóny lze přesměrovat na vybrané IP adresy ○ Požadavky na interní domény lze přesměrovat na řadiče domén nebo jiné autoritativní servery. ○ Přednačítání mezipaměti DNS - záznamy v mezipaměti jsou obnovovány před vypršením jejich platnosti. ○ Záznamy DNS jsou uchovávány v paměti déle, než by autoritativní nameservery pro danou zónu měly být nedostupné z důvodu ttl periody (např. doména.com je nedostupná po dobu jedné hodiny, resolver bude moci použít poslední odpověď, kterou pro tuto doménu měl). ○ DNS firewall - možnost definovat pravidla přístupu pro konkrétní domény - povolení přístupu pouze k vybraným doménám v rámci jedné IP podsítě. Příklad použití -



	povolení přístupu klientských počítačů pouze k doménám Office365, ostatním vrátet odpověď NXDOMAIN. ○ Automatická aktualizace seznamu domén Office365 a dalších služeb Microsoft Azure používaných v bráně firewall DNS. • Centrální management: ○ Zobrazuje provoz DNS v reálném čase ○ Možnost vyloučit určité domény z logování (např. interní domény z důvodu dodržování předpisů). ○ Poskytuje a provádí: ○ Aktualizace databáze na základě filtrování zabezpečení ○ správu aktualizací resolveru a softwaru ○ Centrální úložiště protokolů a incidentů a poskytuje možnosti jejich vyhodnocení. ○ Protokoly o provozu DNS včetně podrobností o všech unikátních požadavcích/odpovědích pro další analýzu jsou přístupné a exportované ze všech resolverů ve společnosti a dostupné včetně fulltextového filtrování v jednom rozhraní (např. ve formátu csv) ○ Možnost analyzovat doménu z hlediska bezpečnosti a obsahu, včetně integrace s bezpečnostními službami třetích stran. ○ Upozornění upozorňující na anomálie zjištěné v provozu DNS pomocí: ○ e-mailu ○ Syslog (TLS) ○ Slack ○ REST API ○ Přehled provozu DNS umožňuje komplexní analýzu komunikace DNS, včetně podrobné: ○ Drilldown jednotlivých událostí ○ filtrování ○ fulltextové vyhledávání ○ export dat ○ přehled trendů v provozu
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na další funkce a komponenty	Whalebone Immunity splňuje všechny požadované vlastnosti, je on-premise, lze plně upravit blokační stránky, aktualizace databáze je dle situace několikrát denně, uvedené formáty pro centrální management jsou podporovány.
Požadavky na Threat intelligence engine	• Pro uživatele má nulovou latenci. Vyhodnocení bezpečnosti je poskytováno v reálném čase. • Nasazení softwaru bez nutnosti nasazení na speciálně upravený hardware, s možností funkce ve virtuálním prostředí. • Ochrana proti útokům typu DNS spoofing na základě DNSSEC včetně podpory NSEC3 a negativního ukládání do mezipaměti. • Možnost definovat různé bezpečnostní politiky a přiřazovat je individuálně dle CIDR anotace nebo přiřazení na základě IP adresy resolveru. • Detekce hrozeb typu Zero-day bez nutnosti předchozí znalosti dané domény • Detekce a upozorňování na anomálie v provozu DNS • Možnost upozornit / zablokovat z vnitřní sítě přístup k doménám, které vypadají podobně jako definovaná doména společnosti/organizace, pro ochranu před cílenými phishingovými útoky • Možnost blokovat přístup k doménám podle kategorie obsahu alespoň v rozsahu: ○ Coinminers ○ P2P připojení (např. torrenty) ○ DNS přes HTTPS (DoH)



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	○ Pornografie ○ Hazardní hry ○ Násilí ○ Tracking ○ Reklama ○ Sociální sítě ○ Hry • Měl by zajistit ochranu proti zneužití provozu DNS k tunelování jiné komunikace v technicky platných paketech DNS a komunikaci s externími servery (zabezpečení tunelování DNS). • Vrstva tunelování DNS proaktivně narušuje tunelování DNS na několika úrovních: ○ Resolver ○ Neuronová síť • Bezpečnostní politiky umožňují nastavení: ○ Úrovně ochrany (blokace) ○ Úrovně detekce (audit) ○ Kategorie hrozeb, které jsou zahrnuty v konkrétních zásadách ○ Vlastní blacklisty a whitelisty ○ Kategorie blokováného obsahu
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na Threat intelligence engine	Ano, Whalebone Immunity disponuje několika neuronovými sítěmi, které vyhodnocují zejména nové hrozby v reálném čase, bez latence pro uživatele. Všechna uvedená nastavení jsou možná.
DNS resolver management	• Poskytuje vzdálenou diagnostiku ○ Monitorování problémů s hardwarem ○ Monitorování softwaru ○ Shromažďování protokolů ○ Vyhodnocení latence překladu • Aktualizace softwaru a zpětné obnovení ○ Možnost okamžitého vrácení provedené aktualizace do předchozího stavu • Místní správa ○ Plný přístup k protokolům pro místní správce ○ Místní rozhraní CLI
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na DNS resolver management	Ano, všechny uvedené parametry Whalebone Immunity splňuje.
Požadavky na Alerting	• Konfigurovatelné filtry pro domény, sítě a akce • Možnosti způsobu doručení alertů včetně: ○ E-mail ○ Syslog (TLS) ○ Slack ○ Webhook (REST API) ○ Další místa doručení výstrah (na vyžádání) • Alerting je založen na: ○ Prahové hodnoty událostí zabezpečení a provozu DNS ○ Detekce dynamických anomálií ○ Whitelisty a blacklisty
Dodavatel stručně popíše způsob	Ano, veškeré uvedené možnosti pro nastavení alertů jsou k dispozici v Administrační konzoli.



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

naplnění jednotlivých požadavků na Alerting	
Požadavky na Ochranu pro zařízení mimo korporátní síť	· Součástí řešení je také aplikace instalovaná lokálně na mobilních zařízeních, která zajistí stejnou úroveň ochrany zařízení, jako by bylo v místní síti pod ochranou lokálního resolveru. · Podporované operační systémy: ○ Windows ○ Android ○ iOS · Možnost hromadného nasazení prostřednictvím zásad skupiny na počítačích spravovaných v doméně (Active directory) · Možnost hromadné instalace na Android / iOS prostřednictvím MDM · Mezi podporované MDM se řadí: ○ Microsoft Intune ○ Sophos ○ A další
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na Ochranu pro zařízení mimo korporátní síť	Ano, Whalebone Immunity disponuje klientem který plní uvedené parametry a umožňuje ochranu i mimo síť zadavatele. Doplněna bude také ochrana pro MacOS zařízení, předpoklad je do konce roku 2025.
Požadavky na reporting	• Zprávy jsou doručovány e-mailem na předem definované adresy. • Možnost nastavení periodicity (7/14/30 dní) a dne v týdnu • Průběžné zprávy shrnují: ○ Objemy DNS provozu ○ Počet hrozeb podle jednotlivých kategorií ○ Podezřelá a infikovaná klientská zařízení ○ Převažující rodiny škodlivých kódů a škodlivých domén
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na reporting	Whalebone Immunity disponuje možností nastavení automatizovaného reportu na zadaný email s uvedenými parametry.
Požadavky na ochranu domény - Identity protection	· Produkt zajišťuje ochranu identit pod vlastní doménou. · hlášení e-mailových adres, které jsou zahrnuty do veřejně známých případů narušení bezpečnosti dat · seznam historických úniků, v nichž figurovaly e-mailové adresy dané domény. · sledování nových úniků a upozorňování na nové úniky · hlášení obsahuje seznam typů citlivých údajů, které figurovaly v úniku (hesla, telefonní čísla, osobní údaje, e-mail, pohlaví, bankovní informace).



**Národní
plán
obnovy**



**Financováno
Evropskou unií**
NextGenerationEU



**MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY**

	· Produkt umožňuje správu incidentů na elementární úrovni - tj. označení incidentu jako vyřešeného/řešitelného. · Produkt obsahuje doporučení, jak daný únik citlivých údajů řešit.
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na ochranu domény - Identity protection	Whalebone Immunity disponuje touto možností, obsahuje jak historické úniky (15 let nazpět), tak novými. V případě nově nalezených úniků dojde k upozornění dle nastavení, přičemž splňuje výše uvedené parametry.
Požadavky na integraci	• Dostupnost rozhraní REST API pro vyhledávání informací pro ○ statistiky provozu DNS ○ Využití REST API požadavků pro filtrování na základě • zdrojové IP adresy • cílové domény • Typ požadavku • Typ hrozby • na IP adresu odpovědi • čas • Monitoring pomocí SNMP ○ Dostupné šablony pro rychlou integraci s monitoringem Zabbix nebo jiným hostitelem SNMP • Integrace protokolu Syslog (SIEM, správa protokolů, provozní monitorování atd.) ○ Konfigurovatelný datový tok prostřednictvím syslogu obsahující zjištěné hrozby ○ Konfigurovatelný datový tok prostřednictvím syslogu obsahující provoz DNS ○ Konfigurovatelná horní část dat prostřednictvím syslogu obsahující bloky z filtrování obsahu ○ Konfigurovatelná top data prostřednictvím syslogu obsahující metriky resolveru a systému
Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na integraci	Ano, Whalebone Immunity plní uvedené zadání, lze takto nakonfigurovat.
Podpora	· 60 měsíců.
Akceptační podmínky	· Veškeré komponenty systému jsou řádně licencované · Bylo dodáno zařízení dle požadované technické specifikace · Všechny komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

	- Byla vytvořena a dodána provozní dokumentace. - Bylo provedeno školení v požadovaném rozsahu
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)	https://www.whalebone.io/cs/immunity https://docs.whalebone.io/cs/latest/ https://www.whalebone.io/cs/materialy-immunity/nove-mesto-na-morave-cz

Implementační služby

Obecné požadavky

Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobcí a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

Zajištění projektového vedení realizace předmětu plnění.

Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení, implementace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

Provedení školení,

Zajištění zkušebního provozu,

Provedení akceptačních testů,

Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

Předání do ostrého provozu,

Dodavatel je dále povinen zahrnout do nabídky i další související potřebné služby nutné pro úspěšnou realizaci díla.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (MS Office) používaných zadavatelem.

Harmonogram realizace

Dodavatel zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky.

HARMONOGRAM

Aktivita	Začátek	Termín
Předání místa plnění	D	D



Národní
plán
obnovy



Financováno
Evropskou unií
NextGenerationEU



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Zahájení projektu – úvodní projektová schůzka - detailní harmonogram včetně návaznosti implementačních prací	D	D+4
Realizace předmětu plnění - implementace kyberbezpečnostních opatření	D+4	D+24
Školení administrátorů	D+24	D+26
Akceptační testy	D+26	D+28
Zahájení ostrého provozu	D+28	-

jednotka = 1 týden

Dodavatel může dle svého uvážení výše uvedené maximální lhůty zkrátit

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

Požadavky na školení

Dodavatel zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

Školení administrátorů – minimální rozsah školení je 8 hodin, předpokládá se účast max. 2 účastníků, školení bude probíhat v sídle Zadavatele.

Školení uživatelů – minimální rozsah školení je 6 hodin, předpokládá se účast max. 5 účastníků, školení bude probíhat v sídle Zadavatele.

Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

S ohledem na pandemii COVID-19 musí být formát školení připraven jak pro prezenční výuku, tak pro možnost provedení školení elektronicky (vzdálenou formou) např. pomocí MS Teams nebo jiných elektronických prostředí pro výuku. Formát školení bude zvolen zadavatelem nejpozději týden před realizací školení, a to podle aktuálního stavu pandemie a dle doporučení relevantních orgánů (Ministerstvo zdravotnictví ČR, Hygienická stanice atp.).

Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

Dodavatel navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování dodavatelem do prováděcí dokumentace.

Dodavatel zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 14 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 7h do 17h. Dojezd do 2 hodin od nahlášení požadavku (v rámci pracovní doby) je zásadní pro udržení provozu kritických informačních systémů v potřebném rozsahu při plnění zákonných povinností zadavatele. V případě předávání díla po částech je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

Požadavky na dokumentaci

Dodavatel zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejich provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

Dodavatel uvede do nabídky kompletní podmínky pro zajištění provozu dodaných prvků, včetně požadavků na aktualizace software (maintenance).

Zhotovitel dále dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele. Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Zhotovitel dále dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat popis správy a údržby dodaného řešení. Dokumentace musí být zhotovena v českém jazyce.

Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Požadavky na záruky a MAINTENANCE

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **60 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Dodavatel ve své nabídce uvede ceny záruky takto:

Standardní záruka a standardní podpora běžně poskytovaná výrobcem infrastrukturní technologie na území České republiky = bude součástí pořizovací ceny zařízení (vždy však alespoň 36 měsíců, není-li výrobcem či dodavatelem poskytnuta jako standardní součást nákupu produktu záruka o délce přesahující 36 měsíců, resp. dosahující minimálně 60 měsíců).

V případě, že výrobce nebo dodavatel neposkytuje jako standardní součást nákupu produktu záruku o délce minimálně 60 měsíců, pak se rozdíl mezi jím nabízenou standardní délkou záruky pro daný produkt a zadavatelem požadovanou délkou záruky minimálně 60 měsíců považuje za nadstandardní (prodlouženou) záruku, kterou je dodavatel povinen k dodávanému produktu (včetně aktualizací software/firmware apod.) pro zadavatele zajistit. Hodnotu takto zajištěné nadstandardní (prodloužené) záruky dodavatel vyjádří v příslušné části cenové kalkulace v položce **"Nadstandardní záruky a podpory výrobců"**.

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

Hlášení záručních závad, řízení a evidence průběhu jejich řešení bude probíhat stejným způsobem a s využitím stejného helpdeskového systému jako u podpory provozu.

Dodavatel nacení i potřebnou MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozování dodaného řešení. Potřebnou maintenance dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.

Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.

Perfekcionista údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

Požadavky na podporu provozu

Obecná pravidla provozu

Pro hlášení servisních požadavků zajistí dodavatel Zadavateli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

Provozní doba helpdeskového systému pro zadávání požadavků musí být 7x24x365.

Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.

Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti

Požadavky na podporu provozu

Rozsah základní technická podpory (ZTP):

Provádění aktualizací firmware a software dodaných produktů (nezahrnuje upgrade na nové hlavní verze software) v rozsahu **8 hodin měsíčně**. Nespotřebované hodiny v měsíci jsou převoditelné do dalších měsíců v rámci příslušného (uhrazeného) roku poskytované technické podpory. Četnost aktualizací řídí Dodavatel s ohledem na zajištění spolehlivého provozu systémů a jejich bezpečnost a kritičnost aktualizací.

Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

Způsob poskytování servisní podpory

Servisní podpora je poskytována zejména následujícím způsobem:

Prostřednictvím pracovníka dodavatele Vzdálenou správou

Prostřednictvím pracovníka dodavatele přímo na pracovišti Zadavatele

Prostřednictvím pracovníka dodavatele formou vzdálené konzultace

Dodavatel provede záznam o provedení servisní podpory, v záznamu uvede relevantní informace včetně doby poskytování servisní podpory a záznam zašle elektronicky zadavateli. Servisní služby,

kteřé jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

Zadavatel je povinen zabezpečit v rámci své součinnosti dodavateli podmínky pro řádné plnění, zejména

- zajistit a udržovat podmínky pro Vzdálený přístup dodavatele,
- zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,
- zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku dodavatele veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,
- umožnit dodavateli v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,
- zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné (na výzvu takovou potřebnost písemně odůvodní).

Dodavatel je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu.

Zadavatel je dále v rámci součinnosti povinen

- elektronicky potvrdit dodavateli provedení služby,
- zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeby a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,
- poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí (pokud tyto nepochází od dodavatele).

Postup při řešení incidentů

Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených v Doplňku SLA, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk).

Součástí nahlášení požadavku Zadavatelem musí být:

- popis Incidentu nebo Požadavku,
- jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu,
- kontaktní osoba.

Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 2 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 7:00 a 17:00 v pracovní dny.

Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.

Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínu vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí,

že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

- v případě Incidentu specifikuje příčinu (pokud je známa),
- vyzve iniciátora k ověření funkčnosti služby.

Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.

Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

Záruky na servisní služby

Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

KYBERBEZPEČNOST
Město Holšov

Položka	Popis položky	Jednotka	Počet jednotek	Jednotková cena v Kč bez DPH	Celková cena v Kč bez DPH	Celková cena v Kč vč. DPH
1 - Systém pro analýzu síťového provozu a bezpečnostní monitoring						
SONDA a KOLEKTOR - SW	GREYCORTEX Mendel perpetualní SW licence: sensor + kolektor / 100Mbps trvalý průtok / 120 obchazených toků za vteřinu & 250 NetFlow za vteřinu / HW server All-in-one model XS / 2x1GBt monitorovací rozhraní / 800GB SSD RAID1 datové úložiště / DELL HW On-Site NBD support	KS	1	1 002 856,00 Kč	1 002 856,00 Kč	1 213 456,18 Kč
IMPLEMENTACE		MD	3	16 000,00 Kč	48 000,00 Kč	58 080,00 Kč
MAINTENANCE support	Průběžná maintenance nutná pro provoz systému	ROK	5	14 900,00 Kč	74 500,00 Kč	90 145,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (4,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (5,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
					1 125 356,00 Kč	1 361 681,18 Kč
2 - ochrana koncových stanic EDR						
Zabezpečení koncových zařízení uživatelů	NGA + EDR ENDPOINTS + SERVERS	KS	150	7 324,00 Kč	499 600,00 Kč	603 306,00 Kč
IMPLEMENTACE	IMPLEMENTACE MD	MD	3	16 000,00 Kč	48 000,00 Kč	58 080,00 Kč
MAINTENANCE support	Průběžná maintenance nutná pro provoz systému	ROK	5	11 600,00 Kč	58 000,00 Kč	70 180,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (4,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (5,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
					604 600,00 Kč	731 566,00 Kč
3 - Systémy vyvíjející kybernetickou bezpečnost - LOG management						
Centralizované logování analýza a report	Centralizované logování analýza a report, LOG management	KS	1	769 589,00 Kč	769 589,00 Kč	931 207,69 Kč
IMPLEMENTACE	IMPLEMENTACE MD	MD	4	16 000,00 Kč	64 000,00 Kč	77 440,00 Kč
MAINTENANCE support	Průběžná maintenance nutná pro provoz systému	ROK	5	12 300,00 Kč	61 500,00 Kč	74 415,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (4,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (5,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
					895 089,00 Kč	1 083 057,69 Kč
4 - INFRASTRUKTURA - datové centrum - nástroj pro zajišťování úrovně dostupnosti Informací						
4a - SERVER	POCET SERVERŮ: 2x server 2x CPU: Intel® Xeon® E5-2680v4 16 fyzických jader / CPU s dvojnásobnou licencí na osm fyzických parametrů serveru (2x procesor s výkonem minimálně 24000 bodů dle http://cpubenchmark.net/ 256GB RAM, 4800MT/s, 2x NVMe SSD 7,68TB / 2x480GB SSD/BASE-T 4x1GBE/záruka 3let NBD	KS	2	423 832,00 Kč	847 664,00 Kč	1 025 673,44 Kč
4b - DISKOVÉ POLE SDS	SDS - softwarově definovaná storage - virtuální storage v každém serveru, Unlimited	KS	1	308 448,00 Kč	308 448,00 Kč	373 222,08 Kč
4c - SERVER OS + CALL	licence HS musí pokrývat všechny CORE v serverech s možností dalšího rozšíření	KS	1	347 212,00 Kč	347 212,00 Kč	420 126,52 Kč
4d - SWITCHÉ CORE	core switch 12x10Gb/SFP+ moduly	KS	2	32 119,00 Kč	64 238,00 Kč	77 727,96 Kč
4e - SWITCHÉ přístupové	SWITCHÉ přístupové 48T x1G	KS	1	84 330,00 Kč	84 330,00 Kč	102 039,30 Kč
4f - NAS + HDD	Minimálně hrubá kapacita/64TB/7200 RPM/10Gb síťový adapter/mezipaměť 2x800GB SSD záruka 3let	KS	1	163 724,00 Kč	163 724,00 Kč	198 106,04 Kč
IMPLEMENTACE a MIGRACE	IMPLEMENTACE a MIGRACE MD	MD	16	16 000,00 Kč	256 000,00 Kč	309 760,00 Kč
MAINTENANCE support	Průběžná maintenance nutná pro provoz systému	ROK	4	7 400,00 Kč	29 600,00 Kč	35 816,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (4,80K projektu)	ROK	1	4 200,00 Kč	4 200,00 Kč	5 082,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (5,80K projektu)	ROK	1	4 100,00 Kč	4 100,00 Kč	4 981,00 Kč
					2 109 116,00 Kč	2 582 314,36 Kč
5 - Ochrana poštovní komunikace, MFA - nástroj pro ověřování identity uživatelů						
5a - MFA	MFA - Multifaktor	KS	100	2 106,60 Kč	210 660,00 Kč	254 899,60 Kč
5b - Ochrana poštovní komunikace	Ochrana poštovní komunikace	KS	1	350 077,00 Kč	350 077,00 Kč	423 593,17 Kč
IMPLEMENTACE	IMPLEMENTACE MD	MD	5	16 000,00 Kč	80 000,00 Kč	96 800,00 Kč
MAINTENANCE support	Průběžná maintenance nutná pro provoz systému	ROK	5	2 890,00 Kč	14 450,00 Kč	16 940,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (4,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč
Nadstandardní záruky a podpory výrobce	Záruky (5,80K projektu)	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč

					654 737,00 Kč	792 231,77 Kč
Ochrana DNS komunikace						
Ochrana DNS komunikace	KS	150	2 452,00 Kč	367 800,00 Kč	445 036,00 Kč	
IMPLEMENTACE	MD	4	16 000,00 Kč	64 000,00 Kč	77 440,00 Kč	
MAINTENANCE support	ROK	5	3 500,00 Kč	17 500,00 Kč	21 175,00 Kč	
Nadstandardní záruky a podpory výrobce	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč	
Nadstandardní záruky a podpory výrobce	ROK	1	0,00 Kč	0,00 Kč	0,00 Kč	
					449 300,00 Kč	543 651,00 Kč
Technická podpora						
Základní technická podpora (ZTP)	ROK	5	228 000 Kč	1 140 000 Kč	1 379 400 Kč	
					1 140 000 Kč	1 379 400 Kč

Cena za dodávku a implementaci řešení KYBERBEZPEČNOST včetně standardní záruky (k doplnění do čl. VI, odst. 2.1. Smlouvy)
Cena za poskytnutí nadstandardní (prodloužená) záruky pro 4, a 5, rok plnění (k doplnění do čl. VI, odst. 2.2. Smlouvy)
Cena za poskytování potřebné maintenance support a Základní technické podpory na 5 let (k doplnění do čl. VI, odst. 2.3. Smlouvy)
CELKOVÁ CENA - kritérium hodnocení (k doplnění do čl. VI, odst. 2. Smlouvy)

bez DPH	s DPH
5 575 200,00 Kč	6 745 992,00 Kč
8 300,00 Kč	10 043,00 Kč
1 395 100,00 Kč	1 688 071,00 Kč
6 978 600,00 Kč	8 444 106,00 Kč

* produkt je nabízen s pěti letou zárukou
Pozn.: Pokud dodavatel nabídne řešení, které je svou podstatou pouze a jen subscription, označí tento produkt ve skupci H parametrem SUBSCRIPTION
Pozn.: Pokud dodavatel nabídne pro některou položku nulovou hodnotu, uveden ve skupci H dle bodu takového ocenění.
Pozn.: Dodavatel před podáním své cenové nabídky ověří správnost výpočtu celkové nabídkové ceny i dle těchto cen.

Příloha č. 3 – Realizační tým

Označení	Pozice	Jméno a příjmení
A.	Projektový manažer	
B.	Technický specialista	
C.	Specialista/konzultant – kybernetická bezpečnost	

Příloha č. 4 – Seznam poddodavatelů

ÚDAJE O PODDODAVATELÍCH	
Požadovaný údaj	Hodnota požadovaného údaje
Dodavatel čestně prohlašuje, že nevyužije k plnění předmětu zadávané veřejné zakázky žádného poddodavatele ve smyslu § 105 zákona.	