Kupní smlouva č. prodávajícího: RCZ-240091
Kupní smlouva č. kupujícího: 27/1/2025

„Dodávka a implementace technologií pro posílení kybernetické bezpečnosti informačních a komunikačních systémů (SIEM, PIM/PAM, servery)“

Prodávající:	Aricoma Systems a.s.
se sídlem:	Hornopolní 3322/34, 702 00 Ostrava
IČO:	04308697
DIČ:	CZ04308697
Spisová značka:	B 11012 vedená u Krajského soudu v Ostravě
zastoupena:	Ing. Zdeněk Chobot, na základě plné moci
bankovní spojení:	Česká spořitelna a.s. 6563752/0800
ID datové schránky:	ctb7phe

(dále jen **„prodávající”** nebo **„dodavatel“**)

a

Kupující:	Statutární město Most
se sídlem:	Radniční 1/2, 434 01 Most
zastoupeno:	Ing. Markem Hrvolem, primátorem
IČO:	00266094
DIČ:	CZ00266094
bankovní spojení:	Česká spořitelna, a.s., č.ú.: 19 - 1041368359/0800
Č. ú. výdajového:	27-1041368359/0800
Č. ú. příjmového:	19-1041368359/0800
e-mail:	posta@mesto-most.cz
ID datové schránky:	pffbfvy

(dále jen „**kupující**“ nebo **„objednatel**“ nebo **„zadavatel“**)

(prodávající a kupující dále také společně jako „**smluvní strany**“)

Shora uvedené smluvní strany se dohodly níže uvedeného dne, měsíce a roku v souladu s § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen "NOZ") na uzavření této

kupní smlouvy (dále jen „**smlouva**”)

I.

Předmět smlouvy

1. Předmět smlouvy je dodávka a implementace technologií pro posílení kybernetické bezpečnosti informačních a komunikačních systémů zadavatele, v souladu se standardy kybernetické bezpečnosti. Součástí předmětu plnění je také poskytnutí servisní a technické podpory po dobu 60 měsíců.

2. Výše uvedený předmět smlouvy je podrobně popsán (specifikován) v zadávací dokumentaci a její příloze č. 7 – Technická specifikace, která je nedílnou součástí této smlouvy (dále jen „**předmět koupě**“).

3. Dodavatel je srozuměn a souhlasí s tím, že zadavatel je oprávněn zrušit předmětnou veřejnou zakázku, v souladu s § 127 odst. 2 písm e) ZZVZ, a s tím související tuto smlouvu, v případě, že mu nebude poskytnuto spolufinancování z Národního plánu obnovy ČR, financovaného Evropskou unií a Ministerstvem vnitra ČR (poskytovatele dotace). Zadavatel je povinen neprodleně poté co zjistí, že mu dotace nebude poskytnuta informovat dodavatele o zrušení veřejné zakázky a tedy o odstoupení (zrušení) od této smlouvy. Odstoupení od smlouvy nastává okamžikem doručení sdělení dodavateli. V případě odstoupení od smlouvy z důvodu neposkytnutí předmětné dotace není dodavatel oprávněn požadovat po zadavateli jakoukoliv náhradu škody (pokud se strany nedohodnou jinak).

4. Smluvní strany jsou srozuměny, že předmětná veřejná zakázka byla vyhlášena a následně zadána v souvislosti s předpokládanou realizací projektu s názvem „Zvýšení kybernetické bezpečnosti Statutárního města Most“, registrační číslo CZ.31.2.0/0.0/0.0/23_093/0008364, který je předložen k poskytnutí finanční podpory z Národního plánu obnovy ČR – komponenty 1.1, 1.2 a 4.4 v rámci výzvy č. 41 - Kybernetická bezpečnost – obce.

5. Realizace projektu uvedeného v předešlém odstavci je vázána dodržováním pravidel v souladu s pokyny vlastníka komponenty 1.1, 1.2 a 4.4 pro příjemce finanční podpory – verze 6 a další platnou legislativou (dále jen „Pokyny“). Pokyny mohou být v průběhu realizace projektu aktualizovány. Pokyny jsou uveřejněna na webových stránkách https://www.mvcr.cz/npo/clanek/dokumenty-programove-dokumenty-programove-dokumenty.aspx Dodavatel je povinen Pokyny v jejich aktuální verzi respektovat.

6. Dodavatel si je vědom skutečnosti, že dílo bude financováno z Národního plánu obnovy ČR, a že porušení podmínek této smlouvy může mít za následek neposkytnutí či krácení této dotace. Dodavatel odpovídá za škodu, která objednateli takto vznikne, a to až do výše ceny díla. V této souvislosti prohlašuje, že se seznámil s podmínkami dotace.

II.

Předání a převzetí

1. Předáním se rozumí okamžik faktického předání předmětu koupě kupujícímu, o čemž se vyhotoví oběma stranami podepsaný předávací protokol. V případě, že na základě dohody dochází zároveň k instalaci na určeném místě, je předání provedeno dovezením na určené místo a zprovozněním není-li výslovně dohodnuto, že zprovoznění není součástí dodávky. V takovém případě bude zároveň sepsán předávací protokol, který bude potvrzen kupujícím.

III.

Kupní cena

1. **Celková kupní cena předmětu koupě** činí: 7.847.030 Kč bez DPH.

   Z toho:

   a) Cena za dodávku PIM/PAM: 1.388.030,- Kč bez DPH (slovy: miliontřistaosmdesátosmtisíctřicet),

   b) Cena za implementaci PIM/PAM: 192.000,- Kč bez DPH (slovy stodevadesátdvatisíce),

   c) Cena za dodávku systému pro správu logů a SIEM: 1.785.000,- Kč bez DPH (slovy: milionsedmsetosmdesátpěttisíc)

   d) Cena za implementaci systému pro správu logů a SIEM: 507.000,- Kč bez DPH (slovy: pětsetsedmtisíc)

   e) Cena za dodávku serverů a implementaci (např. HA, …) vč. technické podpory na dobu 60 měsíců: 1.575.000,- Kč bez DPH (slovy: jedenmilionpěsetsedmdesátpěttisíc)

   f) Cena za technickou podporu PIM/PAM na dobu 60 měsíců: celkem 660.000,- Kč bez DPH (slovy: šestsetšedesáttisíc)

   g) Cena za technickou podporu systému pro správu logů a SIEM na dobu 60 měsíců bez DPH: celkem 1.740.000,- Kč bez DPH (slovy: milionsedmsetčtyřicettisíc)

2. Kupní cena uvedená v odstavci 1 písm. a) až e) je sjednána jako pevná a nepřekročitelná. Uvedená cena bude hrazena na základě jednorázově vystavené faktury způsobem uvedeným v čl. IV. této smlouvy.

3. Kupní cena za technickou podporu (za dostupnost SLA) uvedená v odstavci 1 písm. f), g) bude hrazena měsíčně prostřednictvím faktur vystavených prodávajícím způsobem uvedeným v čl. IV. této smlouvy.

4. Cena s DPH je kalkulována připočtením 21 % k ceně bez DPH, dle aktuální výše sazby DPH v den podpisu smlouvy. Kupující i prodávající jsou povinni při platbě nebo platbách vzít v potaz aktuální výši sazby DPH danou aktuálně platným daňovým předpisem.

5. Zadavatel si vyhrazuje možnost změny závazku ze smlouvy a připouští navýšení nabídkové ceny v průběhu trvání smlouvy v případě zvýšení zákonem stanovené sazby daně z přidané hodnoty dle zák. č. 235/2004 Sb., o dani z přidané hodnoty.

6. V takovém případě bude nabídková cena upravena dle sazeb daně z přidané hodnoty platných v době vzniku zdanitelného plnění za práce neprovedené a nevyfakturované.

7. Kupní cena v sobě zahrnuje náklady spojené s dodáním předmětu koupě, např. náklady na materiály, přepravu, řízení a administrativu, veškeré poplatky spojené s případnou reklamací/servisem a veškeré náklady a výlohy, které jsou nutné k dodání a řádnému zprovoznění předmětu koupě, a to i v případě, kdy tyto nejsou v zadání výslovně uvedeny.

8. Přepravou se rozumí doručení na dohodnuté místo. V případě, že kupující zmaří doručení, je každé další doručování účtováno nad rámec této smlouvy.

IV.

Platební podmínky

1. Úhrady kupní ceny, a to ať už jednorázová úhrada ceny (dle čl. III. odst. 1 písm. a) až e)) či pravidelná dílčí měsíční úhrada ceny technické podpory (dle čl. III odst. 1 písm. f) až g) a odst. 3) bude prodávajícímu uhrazena na základě vystavených daňových dokladů – faktury. Splatnost faktury činí 30 kalendářních dnů od jejího doručení kupujícímu.

2. Daňový doklad (faktura) za dodávky a za implementace bude vystaven do 10 dnů po vzájemném potvrzení akceptačních testů. Daňové doklady (faktury) za technickou podporu (dostupnost SLA) budou vystavovány s měsíční pravidelností, kdy prodávající kupujícímu vždy fakturuje služby, které mu reálně poskytl za předešlý měsíc poskytované služby.

3. Dílčí úhrada za předmět plnění bude objednatelem prováděno vždy na základě skutečně dodaného zařízení či provedení prací a objednatelem odsouhlasených dílčích prací/dodávek a dodavatelem vystavených dílčích faktur.

4. Každá faktura musí obsahovat náležitosti dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, zejména pak:
    a) název, sídlo, IČO a DIČ objednatele a dodavatele
    b) pořadové číslo dokladu
    c) číslo smlouvy objednatele a číslo smluvního vztahu s objednatelem
    d) rozsah a předmět zdanitelného plnění
    e) datum vystavení dokladu
    f) datum uskutečnění zdanitelného plnění
    g) datum splatnosti
    h) cenu bez DPH, DPH a cenu celkem včetně DPH
    i) označení peněžního ústavu a číslo účtu, na který se má platit účtovaná cena
    j) oběma stranami podepsaný protokol o předání a převzetí díla, nebo oběma stranami podepsaný soupis prací
    k) podpis oprávněné osoby
    l) označení „Zvýšení kybernetické bezpečnosti Statutárního města Most“, registrační číslo CZ.31.2.0/0.0/0.0/23_093/0008364, hrazeno z Národního plánu obnovy ČR – komponenty 1.1, 1.2 a 4.4 v rámci výzvy č. 41 - Kybernetická bezpečnost – obce.

Bez kterékoliv z těchto náležitostí konečná faktura nebude proplacena. Dále faktura musí splňovat veškeré podstatné náležitosti dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a dalších zvláštních právních předpisů. Daň z přidané hodnoty bude účtována vždy v souladu s účinnou právní úpravou.

5. Platby dle této smlouvy bude kupující hradit bezhotovostním převodem na účet prodávajícího uvedený v úvodní části této smlouvy. Povinnost kupujícího plnit řádně a včas je splněna připsáním fakturované částky na účet prodávajícího.

6. Kupující je oprávněn před uplynutím lhůty splatnosti vrátit fakturu (daňový doklad) pokud nebude obsahovat uvedené náležitosti. Ve vráceném dokladu musí vyznačit důvod vrácení. Kupující je oprávněn taktéž vrátit fakturu, pokud bude uplatňovat slevu za nedodržení rozsahu technické podpory (dostupnosti SLA) za předešlý měsíc poskytované služby, a to v souladu s čl. VIII. této smlouvy. V takovém případě je prodávající povinen do faktury zahrnout slevu podle vzorce uvedeného v čl. VIII. této smlouvy. Nová lhůta splatnosti počíná běžet od data doručení opravené faktury kupujícímu.

7. Pokud v souvislosti s poskytováním služeb prodávajícím dojde ke vzniku škody kupujícímu nebo třetím osobám, je prodávající povinen bez zbytečného odkladu tuto škodu uhradit uvedením v předešlý stav, není-li to možné, tak ji nahradit v penězích. Veškeré náklady s tím spojené nese prodávající. Prodávající odpovídá i za škodu způsobenou činností těch, kteří pro něj služby poskytují jako jeho pracovníci, subdodavatelé nebo i jinak.

8. Faktury je možné zasílat i v elektronické formě na adresu: faktury@mesto-most.cz.

V.

Dodání, dokumentace, instalace a zprovoznění předmětu koupě

1. Prodávající předá předmět koupě dle čl. II této smlouvy a dle čl. X Harmonogram realizace.

VI.

Podmínky licence

1. V případě, že předmět koupě souvisí s výkonem práva duševního vlastnictví, rozumí se koupí poskytnutí oprávnění k výkonu práva kupujícímu v ujednaném rozsahu. Odměna je v takovém případě součástí kupní ceny uvedené výše.

2. Kupující je oprávněn užívat každou licenci pouze pro vlastní potřebu (organizace, které spravuje odbor informačního systému) a v souladu s jejím určením a za podmínek stanovených zákonem, touto smlouvou a podmínkami stanovenými v licenčním ujednání výrobce.

3. Kupující je oprávněn užívat každou licenci maximálně po dobu platnosti licence, která bude specifikována na dodaném licenčním certifikátu, nebo bude vypočtena od aktivace licence a odvíjí se od data koupě. V případě perpetuální licence je licenci možné používat trvale, bez časového omezení, za předpokladu, že kupující dodržuje všechny podmínky této smlouvy a licenčního ujednání výrobce.

4. Prodávající poskytuje Kupujícímu licenci nevýhradní.

5. Kupující není oprávněn bez předcházejícího písemného souhlasu prodávajícího jakýmkoliv způsobem postoupit, přenechat, zapůjčit, umožnit užívání, či jinak dočasně či trvale poskytnout oprávnění tvořící součást licencí nebo licence třetí osobě, vyjma svých zaměstnanců, kteří ji budou užívat v rámci činností vykonávaných pro kupujícího.

6. Licence udělené na základě této smlouvy, resp. práva a povinnosti přecházejí při zániku Kupujícího na jeho právního nástupce.

7. Doba poskytování licence nebo licencí je specifikována v předmětu koupě. V případě perpetualní licence se doba poskytování licence považuje za neomezenou, za předpokladu, že kupující dodržuje všechny podmínky této smlouvy a licenčního ujednání výrobce.

VII.

Další práva a povinnosti smluvních stran

1. Kupující je povinen uplatnit práva z vadného plnění bez zbytečného odkladu, a to písemně na emailové adrese https://servicedesk.aricoma.com. Prodávající v takovém případě potvrdí kupujícímu, že právo uplatnil na emailovou adresu, ze které uplatnění prodávajícímu přišlo. V tomto emailu mu také sdělí odhadovaný termín opravy.

2. Smluvní strany se dohodly, že prodávající je oprávněn uvádět kupujícího ve svých referencích (a to včetně veřejných zakázek), a to včetně použití informací o předmětu koupě.

3. Hlášení poruch v rámci záručního servisu bude probíhat zasláním požadavku [redacted] či prostřednictvím helpdesku na webových stánkách prodejce https://servicedesk.aricoma.com.

4. Součástí dodávky bude i poskytnutí záruky za jakost a řádnou funkčnost dodaných zařízení podle ustanovení § 2113 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“), jejíž součástí bude i technická podpora a služby (dále jen „záruka“), na dobu 60 měsíců podle čl. VIII Technická podpora a služby.

5. Při požadavku na výměnu disků budou původní nefunkční disky ponechány zadavateli po celou dobu podpory.

6. V případě reklamace diskového pole zůstávají pevné disky u zadavatele

7. komunikace musí probíhat výhradně v českém jazyce.

8. V rámci záruky Dodavatel zaručuje Objednateli řádnou funkčnost dodaného plnění.

9. Řešení nesmí pocházet od společnosti, která je označena, že jejich výrobky HW/SW můžou obsahovat škodlivý kód nebo bezpečnostní riziko.

10. Prodávající vždy nese plnou finanční odpovědnost za případné škody vzniklé v důsledku nedodržení povinností podle čl. VII.

11. Objednatel si v souladu s § 100 odst. 1 ZZVZ vyhrazuje změnu závazku ze smlouvy s vybraným dodavatelem v průběhu plnění předmětu veřejné zakázky, a to výhradu prodloužení doby pro dokončení (změna termínu plnění) z důvodu mimořádně nepříznivých klimatických podmínek nebo nepříznivé situace v souvislosti s vyšší mocí.

12. V případě sporu o oprávněnosti reklamace je dodavatel povinen tuto bez dalšího vyřídit a teprve následně může vůči objednateli uplatnit nárok na úhradu má-li za to, že reklamace byla neoprávněná.

VIII.

Technická podpora a služby

1. Měsíční dostupnost (SLA): 98,00 %. V případě nedodržení měsíční dostupnosti (SLA) dojde ke snížení měsíční ceny technické podpory podle níže uvedené tabulky a vzorce:

Měsíční dostupnost (SLA)	**Sleva z měsíční ceny technické podpory**
97,99 % - 97,00 %	10 %
96,99 % - 95,00 %	15 %
Méně než 95,00 %	30 %

$$Dostupnost\ (\%) = \left(1 - \frac{celkový\ čas\ výpadků\ (minuty)}{\text{celkový čas meření (minuty)}}\right) x100$$

2. Online Helpdesk pro řešení provozních problémů a ohlášených incidentů, který je součástí technické podpory.

3. Technická podpora musí být poskytována výhradně v českém jazyce.

4. Proaktivní údržba, aktualizace a optimalizace systémů je součástí technické podpory.

5. Vzdálený přístup dodavatele do prostředí objednavatele prostřednictvím VPN připojení.

6. Řešení standardních technologických požadavků, například nastavení oprávnění, konfigurační změny, optimalizační úkony.

7. Telefonická asistence dodavatele 9 hodin denně, 5 dní v týdnu je součástí technické podpory.

8. Konzultace k řešení problémů a efektivnímu využívání vybavení je součástí technické podpory.

9. Konzultační a metodická spolupráce při rozvoji, navrhování potřebných opatření a změn je součástí technické podpory.

10. Doby plnění podle níže uvedené tabulky se sankcemi (smluvními pokutami) za jejich nedodržení.[1]

Druhy požadavků	**Zpětná reakce (potvrzení obdržení požadavku)**	**Zahájení zásahu**	**Další specifikace**	**Vyřešení**
Závada	Do 2 hodin od nahlášení nebo zjištění závady	Do 2 hodin od nahlášení nebo zjištění závady	Do 10 hodin od nahlášení nebo zjištění závady, nebude-li dohodnuto jinak	Do 30 hodin od nahlášení nebo zjištění závady, pokud není dohodnuto jinak. Sankce: 100 Kč za každou hodinu prodlení.
Servisní požadavek	Do 2 hodin od nahlášení požadavku	Do 2 hodin od nahlášení požadavku	Do 10 hodin od nahlášení požadavku	Do 50 pracovních hodin od nahlášení požadavku, pokud není dohodnuto jinak. Sankce: 100 Kč za každou hodinu prodlení.
Změnový požadavek	Do 8 hodin od nahlášení požadavku	N/A	Do 10 pracovních dnů od nahlášení požadavku, předložit návrh řešení, pokud není dohodnuto jinak.	Dle dohody. Sankce: 1000 Kč za každý den prodlení.
Požadavek na konzultační služby	Do 8 hodin od nahlášení požadavku	N/A	Do 15 pracovních dnů od nahlášení požadavku,	Dle dohody. Sankce: 1000 Kč za každý den prodlení.

[1] Doby plnění se počítají pouze v pracovní době systému (pracovní hodiny) od 8:00 do 17:00. Pro účely sankcí se délka prodlení počítá také pouze v pracovní době.

			poskytnout konzultaci, pokud není dohodnuto jinak.	

- Pokud bude rozsah závady takový, že nebude možné provést nápravu obvyklými prostředky, musí dodavatel do 24 hodin od nahlášení závady navrhnout náhradní řešení, jehož realizaci objednatel bezodkladně zváží s ohledem na možné poškození jeho zájmů.
- Zajištění záručního servisu technologií nebo předmětu plnění je součástí technické podpory.
- Cena technické podpory zahrnuje pravidelné profylaxe prostředí a to minimálně jednou ročně.
- Cena technické podpory zahrnuje bezodkladné aktualizace prostředí v případě zjištění bezpečnostní hrozby, která může ohrozit informační systém objednatele (všechny komponenty, které využívá aplikační prostředí, a nejsou součástí operačního systému, který si sám aktualizuje zadavatel VZ). Bude klasifikováno podle SLA jako závada.
- Určení druhu požadavku náleží objednateli.
- Servisní požadavky budou plněny přednostně v pracovní době (pracovní dny od 8:00 do 17:00), v takovém případě je cena za jejich plnění součástí ceny technické podpory.

Cena technické podpory zahrnuje všechny náklady na poskytování technické podpory, včetně nákladů spojených s technickou podporou a garancí nástupu servisního technika (zahájení zásahu).

IX.

Smluvní pokuty

1. V případě prodlení prodávajícího s dodáním bezvadného předmětu koupě, je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 0,5 % z kupní ceny za každý započatý den prodlení.

2. V případě, že prodávající poruší některou z povinností stanovenou mu v čl. VIII – Technická podpora a služby, je kupující oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč za každé takovéto porušení. Uvedená výše smluvní pokuty se netýká případů uvedených v tabulce v odstavci 10 čl. VIII smlouvy, pro uvedené případy platí smluvní pokuty tam uvedené.

3. Vznikem povinnosti hradit smluvní pokutu ani jejím faktickým zaplacením není dotčen nárok na náhradu škody v plné výši. Odstoupením od smlouvy nárok na již uplatněnou smluvní pokutu nezaniká. Smluvní pokuta je splatná deset dnů po doručení písemného oznámení o jejím uplatnění druhé smluvní straně. Smluvní strany shodně prohlašují, že s ohledem na charakter povinností, jejichž splnění je zajištěno smluvními pokutami, a dále s ohledem na charakter předmětu koupě a zájem na jeho řádném a včasném provozu považují smluvní pokuty uvedené v tomto článku za přiměřené.

4. V případě, že se ukáže, že prohlášení dodavatele dle čl. XII odst. 15 Smlouvy je v rozporu s realitou (tedy dodavatel uvede nepravdivé údaje), případně dodavatel neprodleně (nejpozději do 5 pracovních dnů od doby co se informaci dozvěděl) nesdělí změnu okolností dle čl. XII odst. 16 Smlouvy, tak je objednatel oprávněn požadovat po dodavateli smluvní pokutu ve výši 20.000,- Kč za každé takové jednotlivé pochybení.

5. V případě prodlení kupujícího se zaplacením kterékoliv části kupní ceny, která přesáhne 5 pracovních dní, je kupující povinen uhradit prodávajícímu smluvní pokutu ve výši 0,5 % z kupní ceny za každý den prodlení.

X.

Harmonogram realizace

1. 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.

2. Zadavatel vyžaduje navržení následujícího harmonogramu plnění – kde dodavatel uvede maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo, čísla značí počet kalendářních dnů. Celková aktivita projektu musí být v souladu s podmínkami Výzva č. 41 - Kybernetická bezpečnost – pro obce zNárodního plánu obnovy a nesmí je překročit, musí být dokončena v dostatečném předstihu, a to nejpozději **do 34 týdnů od nabytí účinnosti smlouvy**.

Poř. č.	**Aktivita projektu**	**Nejpozdější termín pro dokončení aktivity**
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+90
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+110
E1.4	Dodávky a implementace	D+170
E1.5	Školení uživatelů a administrátorů	D+190
E1.6	Zkušební provoz	D+200
E1.7	Akceptační testy	D+220

~~3.~~ Dodavatel musí zohlednit bod 4.1. Fáze plnění v příloze ZD č. 7 - Technická specifikace.

XI.

Ustanovení o zániku smlouvy

1. Kupující je oprávněn od této smlouvy odstoupit dle zákonem stanovených důvodů nebo důvodů v této smlouvě uvedených.

2. Prodávající je oprávněn od této smlouvy odstoupit v případě, že kupující bude v prodlení s úhradou svých peněžitých závazků vyplývajících z této smlouvy po dobu delší než třicet dnů. Kupující je oprávněn od této smlouvy odstoupit v případě, že předmět koupě nebude splňovat podmínky sjednané v VII. bodě této smlouvy bude zjištěn rozpor s těmito ujištěními.

3. Každé odstoupení od této smlouvy musí mít písemnou formu, přičemž písemný projev vůle odstoupit od této smlouvy musí být druhé smluvní straně doručen doporučeným dopisem na adresu specifikovanou v záhlaví této smlouvy.

4. Účinky každého odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně. Odstoupení od smlouvy se nedotýká nároku na náhradu škody vzniklé porušením této smlouvy ani nároku na zaplacení smluvních pokut.

5. V případě odstoupení od smlouvy si strany vzájemně vypořádají závazky z této smlouvy, tedy dojde k případnému vyúčtování již plněného závazku, to neplatí v případě odstoupení dle čl. IX.4. V případě, že se strany na vypořádání závazků neshodnou, tak si v souladu se zákonem vzájemně vrátí to, co již bylo na základě této smlouvy plněno (hrazeno).

XII.

Závěrečná ustanovení

1. Obsah smlouvy může být měněn nebo doplňován po předchozí dohodě stran. Jakékoliv dodatky/změnové listy smlouvu měnící, rozšiřující nebo doplňující její ustanovení, musí být uzavřeny v písemné formě, očíslovány v postupné řadě za sebou počínaje číslem 1 a podepsány.

2. Prodávající může samostatně před uplynutím licencí, jsou-li také předmětem koupě, nabízet kupujícímu prodloužení práva nebo aktualizaci užití předmětu koupě. Prodávající je také oprávněn nabízet kupujícímu rozšíření k danému předmětu koupě. Kupující není

povinen takovouto nabídku přijmout. Nepřijetím takové nabídky nezaniká právo kupujícího užívat stávající licence.

3. Smlouva je vyhotovena ve 2 stejnopisech, z nichž 1 obdrží objednatel a 1 dodavatel v případě listinné formy smlouvy.

4. Smlouvu je možno měnit pouze na základě dohody formou písemných číslovaných dodatků podepsaných zástupci obou smluvních stran.

5. Obě strany se zavazují, že veškeré případné spory, do nichž se při plnění této smlouvy dostanou, budou řešeny v prvé řadě dohodou. Zástupci smluvních stran se sejdou na základě písemné výzvy v dohodnutém termínu a místě nejpozději do 10 dnů ode dne doručení výzvy.

6. Sjednává se, že smluvní strany považují povinnost doručit písemnost do vlastních rukou za splněnou i v případě, že adresát zásilku, odeslanou na jeho v této smlouvě uvedenou či naposledy písemně oznámenou adresu pro doručování, odmítne převzít, její doručení zmaří nebo si ji v odběrní lhůtě nevyzvedne, a to desátým dnem ode dne vypravení písemnosti.

7. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla vedena v evidenci smluv vedené statutárním městem Most, kde bude přístupná dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a která obsahuje údaje o smluvních stranách, předmětu smlouvy, číselné označení této smlouvy a datum jejího uzavření.

8. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství a udělují svolení k jejich zpřístupnění ve smyslu zákona č. 106/1999 Sb. a zveřejnění bez stanovení jakýchkoli dalších podmínek.

9. Tato smlouva podléhá uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany se dohodly, že smlouvu v souladu s tímto zákonem uveřejní kupující, a to nejpozději do 30 dnů od podpisu smlouvy. V případě nesplnění tohoto ujednání může uveřejnit smlouvu v registru prodávající.

10. Po uveřejnění v registru smluv obdrží prodávající elektronickou poštou od kupujícího potvrzení z registru smluv. Potvrzení obsahuje metadata, je ve formátu .pdf, označeno uznávanou elektronickou značkou a opatřeno kvalifikovaným časovým razítkem.

11. Při nakládání s osobními údaji se smluvní strany řídí Nařízením 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 (obecní nařízení o ochraně osobních údajů) a zákonem č. 110/2019 Sb., o zpracování osobních údajů ve znění pozdějších předpisů a dále pak ID_ST_076 Nakládání s osobními údaji.

12. Smluvní strany prohlašují, že ujednání v této smlouvě obsažená jsou jim jasná a srozumitelná, jsou jimi míněna vážně a byla učiněna na základě jejich pravé a svobodné vůle. Na důkaz tohoto tvrzení smluvní strany připojují níže své podpisy.

13. Strany sjednávají, že veškeré spory vyplývající z této smlouvy, které nebude možno vyřešit smírnou cestou, budou řešeny v rámci místní příslušnosti Okresním soudem v Mostě. V případě, že bude v prvním stupni věcně příslušný krajský soud, sjednávají smluvní strany místní příslušnost Krajského soudu v Ústí nad Labem.

14. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv.

15. Dodavatel prohlašuje, že jeho obchodní společnost není obchodní společností (osobou), ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů (tj. člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády) nebo jím podíl představující alespoň 25 % účasti společníka v obchodní společnosti ovládaná osoba vlastní;

    a) poddodavatel (subdodavatel), prostřednictvím kterého dodavatel prokazuje kvalifikaci (existuje-li takový), není obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů (tj. člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka
    b) v obchodní společnosti;
    c) dodavatel (případně poddodavatel) dále čestně prohlašuje, že se na něj nevztahuje nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, dle kterého není možné zadat veřejnou zakázku:

        i. jakémukoli ruskému státnímu příslušníkovi, fyzické či právnické osobě nebo subjektu či orgánu se sídlem v Rusku,

        ii. právnické osobě, subjektu nebo orgánu, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo

iii. fyzické nebo právnické osobě, subjektu nebo orgánu, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce, včetně poddodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky, nebo společně s nimi.

Dodavatel (případně poddodavatel) dále čestně prohlašuje, že žádné finanční prostředky, které obdrží za plnění veřejné zakázky, dodavatel nepoužije v rozporu s mezinárodními sankcemi podle § 2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů, zejména, že tyto finanční prostředky přímo ani nepřímo nezpřístupní osobám, subjektům či orgánům s nimi spojeným uvedeným v sankčních seznamech v souvislosti s konfliktem na Ukrajině nebo jejich prospěch; aktuální seznam sankcionovaných osob je uveden na https://www.financnianalytickyurad.cz/files/20220412-ukr-blr.xlsx.

16. Dodavatel je povinen neprodleně informovat objednatele v případě, že se v jeho obchodní společnosti případně u některého poddodavatele vyskytnou okolnosti, které by byly v rozporu s podmínkami stanovenými v čl. X odst. 15 této Smlouvy či v rozporu s platnými právními předpisy ČR či předpisy Evropské unie, které upravují výše uvedenou problematiku (tedy zejména problematiku střetu zájmů a opatření související s válkou na Ukrajině).

17. Při nakládání s osobními údaji se strany řídí Nařízením 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), zákonem č. 110/2019 Sb., o zpracování osobních údajů.

18. Dodavatel je v rámci realizace díla povinen naplňovat podmínky udržitelného rozvoje a postupovat v souladu s čl. 9 nařízení Evropského parlamentu a Rady (EU) 2021/1060 (dále „Obecné nařízení“) a dodržovat zásadu „významně nepoškozovat“ environmentální cíle (dále jen DNSH) ve smyslu článku 17 nařízení Evropského parlamentu a Rady (EU) 2020/852. Další povinnosti plynoucí z povinnosti plnění DNSH, kterými je Dodavatel vázán, jsou popsány v Pokynech vlastníka komponent 1.1, 1.2 a 4.4 pro příjemce finanční podpory. Pokyny jsou uveřejněna na webových stránkách https://www.mvcr.cz/npo/clanek/dokumenty-programove-dokumenty-programove-dokumenty.aspx

19. Dodavatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů. Dodavatel je povinen poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského

účetního dvora (dále také „EÚD“), Nejvyššího kontrolního úřadu (dále také „NKÚ“), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost, a to minimálně do 31. 12. 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí být použita delší lhůta.

20. Dodavatel je povinen archivovat uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu této smluv minimálně do 31. 12. 2036. Pokud je v českých právních předpisech stanovena lhůta delší, musí být použita pro úschovu delší lhůta.

21. Dodavatel prohlašuje, že neporušuje etické principy, principy společenské odpovědnosti ani základní lidská práva.

22. Dodavatel je povinen zajistit řádné a včasné plnění finančních závazků svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení (vyjma případných sjednaných pozastávek) poddodavatelem řádně vystavených a doručených faktur za plnění poskytnutá k plnění veřejné zakázky, a to vždy do 10 pracovních dnů od obdržení platby ze strany objednatele za konkrétní plnění. Dodavatel se zavazuje přenést totožnou povinnost do dalších úrovní dodavatelského řetězce a zavázat své poddodavatele k plnění a šíření této povinnosti též do nižších úrovní dodavatelského řetězce.

23. Nedílnou součástí této smlouvy se stává:
Příloha č. 1 – Technická specifikace

V Mostě dne:

[redacted]

za statutární město Most
Ing. Marek Hrvol, primátor města
kupující

V Teplicích dne:

[redacted]

……..
za Aricoma Systems a.s.
Ing. Zdeněk Chobot, ředitel RC
prodávající

Příloha č. 1 – technická specifikace

1 Podrobný popis předmětu plnění

1) Předmětem plnění této veřejné zakázky je dodávka a implementace technologií pro posílení kybernetické bezpečnosti informačních a komunikačních systémů zadavatele, v souladu se standardy kybernetické bezpečnosti (dále jen „dodávka“, „systém“, „řešení“ nebo „technologie“). To zahrnuje také všechny nezbytné služby. Detailní specifikace dodávek a služeb jsou uvedeny v dalších kapitolách tohoto dokumentu. Součástí plnění je rovněž zajištění provozu (údržby) po dobu minimálně 60 měsíců od předání řešení do ostrého provozu. Řešení musí být navrženo s ohledem na minimalizaci nákladů na provoz systémů.
2) U technických parametrů, u nichž není explicitně uvedeno, že se jedná o minimální nebo maximální požadovanou hodnotu, je možné nabídnout i řešení s lepšími parametry, tedy řešení, která překračují stanovené požadavky ve smyslu výhodnějších užitných hodnot, pokud zadávací podmínky nevyžadují striktní dodržení specifických hodnot.
3) Předmětem plnění veřejné zakázky jsou zařízení a systémy uvedené v následující tabulce, včetně souvisejících služeb a položek:

Položka	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
P.1	Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS Magistrátu města Mostu (dále jen MmM)	1. Zavedení nástroje pro správu a řízení oprávnění privilegovaných účtů správců IS - zaměstnanců MmM a externích uchazečů - při vzdáleném i lokálním přístupu k IS. 2. Součástí je pořízení software pro správu privilegovaných účtů a přístupů, dále implementace a související služby.	soubor	1
P.2	Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management, SIEM)	1. Zaznamenávání činností (logů) z datových center, virtuálních serverů, firewallů, switchů atd. a souvisejících systémů do externích systémů. 2. Nástroje pro kompletní správu životního cyklu (pořízení, zpracování, zobrazení, prohledávání, ochrana, uchování	soubor	1

		a archivace) logů chráněných IS a souvisejících a podpůrných systémů a technologií. 3. Nasazení nástroje auditování činností uživatelů a administrátorů. 4. Pokročilé notifikační nástroje bezpečnostních a nestandardních událostí. 5. Analýza KBU a identifikace možných KBI		
P.3	Nástroje pro zajišťování úrovně dostupnosti informací – HW pro zajištění provozu implementovaných řešení	1. Dva nové servery, vysoká dostupnost, Software-defined storage (SDS) 2. Management server. 3. Licence	soubor	1

2 Požadované parametry technického řešení

2.1 Obecné požadavky

(1) Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje princip technologické neutrality, tj. využívá technologie způsobem, který neomezuje implementaci technologií různých výrobců. Tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.

(2) Pokud účastník vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na těchto konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(3) Pokud navržené řešení účastníka vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.), která není součástí popisu předmětu plnění, účastník musí do své ceny zahrnout všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

(4) Pro každý softwarový produkt nabídnutý v rámci řešení budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně specifikace konkrétní infrastruktury, na které bude řešení provozováno.

(5) Dodavatel je povinen poskytnout řešení, které umožňuje efektivní připojení a správu více domén Active Directory (AD) z různých afiliovaných entit, např. GOV (MmM) a EDU (MŠ) licence. Řešení musí splňovat následující specifické požadavky:

a. Podpora Více Domén:
    i. Řešení musí umožnit integraci a centralizovanou správu více domén v rámci jedné infrastruktury.
    ii. Musí zahrnovat možnosti pro správu uživatelských účtů, skupin a politik napříč těmito doménami.
b. Podpora Různých Afiliací:
    i. Řešení musí být kompatibilní s různými typy afiliovaných entit, jako jsou např. GOV a EDU licence, a musí splňovat licenční požadavky pro tyto typy institucí.
    ii. Dodavatel musí poskytnout podrobnosti o licenčních podmínkách a o tom, jak budou tyto podmínky aplikovány na integraci a správu domén.
c. Multiplexing a Licencování:
    i. Řešení musí dodržovat všechny licenční požadavky související s multiplexingem, který může být použit pro sdílení přístupu mezi více uživateli nebo zařízeními.
    ii. Dodavatel musí zajistit, že multiplexing není použit k obcházení licenčních podmínek a že každé připojení a použití softwaru je správně licencováno.
    iii. Součástí nabídky musí být dokumentace popisující způsob, jakým je multiplexing podporován a jak jsou splněny licenční požadavky.
d. Náklady:
    i. Řešení nesmí generovat žádné dodatečné finanční náklady nad rámec sjednané ceny za dodávku a implementaci. To zahrnuje všechny náklady spojené s integrací, správou více domén a různými afiliacemi, včetně licenčních poplatků.
    ii. Dodavatel je povinen zajistit, že všechny související náklady jsou zahrnuty v celkové ceně nabídky a že nebudou vyžadovány žádné dodatečné platby v průběhu implementace a používání řešení.

(6) Účastník musí používat stávající prostředky a technologie, aby snížil náklady a usnadnil správu. Pokud potřebuje funkce podobné těm, které už jsou k dispozici, musí využít stávající prostředky a případně je rozšířit, místo zavádění nových platforem nebo služeb, např. jako jsou nové virtualizační platformy nebo adresářové služby.

(7) Účastník prokáže, že všechny dodávky, které dodá zadavateli:
a. jsou nové, oprávněně uvedené na trh v EU nebo pocházejí z autorizovaného prodejního kanálu výrobce,
b. mají plnou záruku od výrobce,
c. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
d. obsahují licenci na používání příslušného softwaru,
e. jsou určeny pro provoz v České republice,
f. z databáze výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti účastník doloží čestným prohlášením distributora nebo, pokud není možné získat prohlášení distributora, vlastním prohlášením účastníka. Zadavatel si vyhrazuje právo na ověření původu výrobku při jeho převzetí na základě příslušných sériových čísel a právo podpisu akceptačního protokolu, který osvědčuje převzetí dodávky až po ověření původu výrobku.

2.2 Specifické požadavky – P1 – Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS MmM

(1) Cílem zadavatele veřejné zakázky je pořízení systému pro řízení a správu privilegovaných účtů (dále jen PIM/PAM), který zajistí jednotnou správu přístupu k privilegovaným účtům a monitorování operací prováděných pod těmito účty, včetně vazby na konkrétního administrátora, který v danou chvíli účet používá. Systém musí zahrnovat dvoufaktorovou autentizaci a poskytnout podrobné školení pro IT pracovníky zadavatele veřejné zakázky ohledně správy dodaného systému.

(2) V současnosti je správa většiny prvků IS a KS zadavatele veřejné zakázky prováděna externími subjekty na základě servisní smlouvy. Tito specialisté/správci přistupují k prvkům vzdáleně, převážně prostřednictvím VPN. Přihlášení správce do VPN je zaznamenáváno, ale jeho další činnost v IS již monitorována ani zaznamenávána není (kromě běžného logování v jednotlivých prvcích, pokud je prováděno) a ani řízena. Většina správců disponuje privilegovanými účty, tj. účty s vysokými (administrátorskými) oprávněními ke spravovaným a souvisejícím prvkům. Zadavatel veřejné zakázky nemá kontrolu nad správou a využíváním těchto účtů u jednotlivých subjektů.

(3) Z hlediska bezpečnosti umožňují privilegované účty téměř neomezený přístup a manipulaci s informačními aktivy organizace. V případě kompromitace takového účtu je organizace vystavena vysokému riziku zneužití, vyzrazení informací nebo jejich zneužití.

(4) Důležitou požadovanou oblastí je detailní audit užití a aktivity privilegovaných účtů. Aktivita bude zaznamenávána nahráváním uživatelských relací prostřednictvím tzv. „jump serveru“, což zahrnuje snímání obrazovky a logování uživatelského vstupu (key-logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu bude nahrávána ve video formátu a jednoznačně přiřazena konkrétní osobě. Nahrávky budou zabezpečeným způsobem přenášeny do centrálního úložiště, kde budou dlouhodobě uchovávány a kontextově vyhledatelné. Tyto nahrávky budou klíčovým důkazem pro prokázání veškeré aktivity uživatele. Součástí bude také zajištění auditní stopy správy privilegovaných účtů.

(5) Implementace systému bude provedena v souladu s § 19 Správa a ověřování identit Vyhlášky č. 82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

(6) Požadavek řídit privilegované účty je hlavním požadavkem zákona o kybernetické bezpečnosti (ZKB) a standardů kybernetické bezpečnosti. Tento požadavek se týká zajištění bezpečnosti informačních systémů, nejen těch, které jsou označeny jako významné informační systémy (VIS) nebo informační systémy kritické informační infrastruktury (IS KII). Nesplnění těchto požadavků může vést k sankcím ze strany Národního bezpečnostního úřadu, který provádí audity zaměřené na posouzení souladu se ZKB a VKB.

(7) Součástí dodávky bude vybudování monitorovaného serveru/appliance, který bude sloužit pro provádění vzdálené správy externími partnery. Veškerá činnost těchto partnerů bude zaznamenávána. Server bude bezpečně publikován do internetu prostřednictvím stávajícího firewallu, a veškerá komunikace probíhající přes internet musí být šifrována bez potřeby využití VPN apod.

2.3 Specifické požadavky – P2 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management, SIEM)

(1) V současné době nevlastní zadavatel veřejné zakázky žádný nástroj pro (centrální) zaznamenávání činnosti (logů) a navazujících systémů. Činnosti jsou v některých systémech zaznamenávány lokálně, ale bez jednotné politiky, dlouhodobého ukládání a ochrany logů před změnou, přetečením apod. Chybí nástroj pro podporu řešení případných kybernetických událostí a incidentů, poskytování konsolidovaných informací před vznikem a v průběhu události/incidentu. Absence nástroje rovněž neumožňuje efektivně analyzovat chování IS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezení jeho opakování.

(2) Zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců bude dosaženo: Implementací nástroje pro správu logů (tzv. log management) – zavedením komplexního systému pro správu logů dojde k centralizovanému sjednocení různých bází bezpečnostních a provozních záznamů, které jsou poskytovány různými typy hardwarových zařízení, provozovanými operačními systémy a aplikacemi, včetně všech nástrojů implementovaných v rámci tohoto projektu. Zaznamenané činnosti budou k dispozici na jednom místě ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 18 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby. Systém musí zajistit integritu archivu.

(3) Požadované řešení je standardní Log/Event Management, který bude napojen na SIEM systém, který je součástí dodávky a jako celek musí umožňovat napojení na služby SOC (Security Operations Center).

(4) Řešení musí umožnit sofistikovanou, transparentní a opakovatelnou pokročilou analýzu spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů.

(5) Nabízené řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

(6) Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů a podporu běžného provozu komplexního řešení ICT infrastruktury zadavatele veřejné zakázky.

(7) Pro zajištění požadavků bezpečnosti musí řešení Log/Event Management disponovat konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům.

(8) Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 3 měsíce) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.
(9) Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.
(10) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze HTTPS bez nutnosti instalace klienta. Ukládání všech informací bude prováděno do jedné databáze (nebo více integrovaných databází), tak, aby bylo možné realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů.
(11) Mandatorní informace, které budou v systému vždy obsaženy a uchovány, jsou vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.
(12) Řešení bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopné dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.
(13) Implementace systému bude provedena v souladu s § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí Vyhlášky č. 82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.
(14) Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině.
(15) Zadavatel veřejné zakázky bude vyžadovat poskytnutí funkčního vzorku (v identické konfiguraci s nabízeným systémem) pro účely testování a ověření požadovaných funkčních vlastností. Účastník je povinen doručit testovací vzorky na místo plnění do pěti (5) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný účastník poskytne testovací vzorky bezplatně a na dobu minimálně následujících 30 pracovních dnů poskytne i součinnost s testováním.
(16) Zadavatel veřejné zakázky v rámci testovacího provozu na dodaném testovacím vzorku, vycházeje z dodané dokumentace k nabízenému systému, provede tyto práce a vytvoří záznam o jednotlivých činnostech a jejich výsledcích. Jedná se zejména o tyto testy:
    a. Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele veřejné zakázky, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému.
    b. Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele veřejné zakázky a otestování následujících vlastností:
        i. Nastavení klasifikace zdrojů.
        ii. Nastavení značek (tagů) pro vybrané zdrojové systémy.
        iii. Filtrování událostí.
        iv. Úprava normalizace existujícího zdroje v grafickém rozhraní nástroje.
        v. Vytvoření reportů a exportu logů a vybraných údajů z logů.

c. Konfiguraci pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému.
d. Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému – viz Technická specifikace, všechny body z odstavce „Sběr událostí z Microsoft prostředí“ včetně centrální instalace a centrální konfigurace Microsoft Sysmon služby pro rozšíření hodnoty logů vytvářených zdrojovými systémy dle doporučené auditní politiky.
e. Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele veřejné zakázky v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran.
f. Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
    i. Provedení zálohy konfigurace a dat na externí systém.
    ii. Vytažení dvou libovolných disků za běhu systému.
    iii. Nastavení systému do továrního nastavení.
    iv. Obnovení konfigurace a všech dat z vytvořených záloh.
    v. Kontrola úplnosti obnovené konfigurace a dat ze záloh.
    vi. Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat.
    vii. Kontrola výkonu systému v běžné zátěži – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace.
    viii. Kontrola kompletnosti dokumentace pro nabízený systém v českém jazyce.

Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného funkčního vzorku systému dle Technické specifikace tohoto zadání.

2.4 Specifické požadavky – P3 – Nástroje pro zajišťování úrovně dostupnosti informací – HW pro zajištění provozu implementovaných řešení

(1) Pro provoz kyberbezpečnostních řešení (Logování, PIM-PAM, SIEM) pořizovaných v rámci projektu bude pořízen výkonný HW, který zajistí vysokou dostupnost provozovaných řešení a zároveň zajistí dostatečný výkon. Z hlediska bezpečnosti se bude jednat o zcela samostatnou infrastrukturu (blackbox), která bude mít min. nebo žádnou vazbu na stávající systémy.
(2) Veškerý provoz bude konsolidován na 2 nody (hypervisory) s dostatečným výkonem i diskovou kapacitou. Pro ideální využití diskového prostoru v jednotlivých nodech bude nasazeno tzv. SDS (softwarově definované storage) řešení

využívající interní diskovou kapacitu jednotlivých nodů. SDS řešení bude integrováno do nabízené virtualizační vrstvy. Celková využitelná kapacita ze všech nodů SDS musí být min. 73 TB SATA (SAS rozhraní) vrstvě, tato vrstva bude akcelerována čtecími i zapisovacími operacemi o kapacitě min. 7 TB.

(3) Nody musí být zapojeny redundantně do dvou datacenterových LAN přepínačů. Celá infrastruktura bude využívat LAN o rychlosti min. 10GbE.

(4) Celé prostředí musí být zalicencované v poslední (aktuální) edici. V případě operačního systému Windows musí být zalicencované v edici 2025 (perpetualní licence).

2.5 Specifické požadavky – povinné parametry řešení

(1) V dále uvedených tabulkách jsou uvedeny minimální požadované (povinné) parametry dodávaného řešení.

(2) Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Účastník tedy uvede konkrétní technické parametry nabízeného zboží, včetně uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.

(3) Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku zadavatele), že nabízené řešení jednoznačně splňuje všechny požadavky.

(4) Účastník musí všechny povinné parametry splnit, v případě nesplnění bude jeho nabídka vyloučena.

(5) Požadavky na zvýšení zabezpečení komunikační sítě:

Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS

Část	Parametr	Popis povinného parametru	Naplnění povinného parametru	Odkaz na část nabídky, kde je možné ověřit naplnění parametru
PIM/PAM systém	Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.	Wallix PIM/PAM (dále jen WPP) umožňuje centrální správu přístupových práv k privilegovaným účtům, včetně monitorování relací, auditu a záznamu aktivit. Přístup je řízen podle zásad "nejmenší nutné oprávnění" a přiřazen podle uživatelských rolí.	zde
	Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.	WPP podporuje multi-tenant architekturu, která zajišťuje, že přístupy jednotlivých uživatelů, včetně administrátorů, jsou omezeny jen na povolené složky, účty a konfigurace.	zde
	Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových	WPP umožňuje víceúrovňové schvalování přístupů, kde přístupy mohou být omezeny podle účtu nebo časového úseku. Schvalování může být vynuceno pro přístup k přihlašovacím údajům nebo k připojení na koncový systém. Uživatelé jsou	zde

		žádostech, schválení a zamítnutí budou uživatelé upozornění emailem nebo vytvořením ticketu v helpdesk systému.	informováni o nových žádostech, schváleních a zamítnutích prostřednictvím emailu nebo ticketu v helpdesk systému.	
	Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaných přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi.	WPP používá šifrovací algoritmy AES-256 a SHA2 pro ochranu dat a záznamů. Ukládání citlivých informací v centrální databázi splňuje požadavky GDPR, PCI-DSS a dalších regulací.	zde
	Jednotná centrální správa	Správa řešení je umožněna pomocí jednotné centrální správy.	WPP poskytuje jednotnou centrální správu, která umožňuje efektivní řízení všech aspektů řešení z jednoho místa.	zde
	Podpora MS Active Directory	Řešení musí podporovat plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.	WPP plně podporuje integraci s Microsoft Active Directory, včetně informací o uživatelích, skupinách a emailech. Integrace umožňuje mapování rolí v PAM řešení na základě skupin v AD.	zde
	Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML).	WPP poskytuje přístup k uživatelskému rozhraní přes webový portál, který podporuje ověření přes LDAP/MS Active Directory a druhý faktor, jako je LDAP, Radius server nebo SAML.	zde
	Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou	WPP umožňuje vynutit silnou autentizaci uživatelů, která zahrnuje kombinaci jména/hesla a druhého faktoru, jako je	zde

		autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, LDAP, SAML, atp...). Řešení nabízí vlastní MFA nástroj, nebo bude součástí nabídky MFA třetí strany.	RADIUS, LDAP nebo SAML. Řešení nabízí vlastní nástroj pro multi-faktorovou autentizaci (MFA) nebo integraci s MFA třetí strany.	
	Šifrování a zabezpečení dat	Řešení musí splňovat šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA, atd.	WPP splňuje šifrovací standardy AES-256 a RSA-2048, což umožňuje společnostem splnit požadavky na compliance pro ZKB, GDPR, PCI-DSS, SOX, HIPAA a další.	zde
	Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i správcem PIM/PAM řešení. Hesla a SSH klíče se vyměňují bezagentově. Řešení musí podporovat změnu přihlašovacích údajů, zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele.	WPP umožňuje automatickou výměnu hesel a SSH klíčů po ukončení relace nebo v pravidelných intervalech podle bezpečnostní politiky. Rotaci lze vynutit i správcem řešení. Výměna hesel a SSH klíčů probíhá bezagentově a řešení podporuje customizaci password management modulu pro další systémy.	zde
	Ukládání hesel	Řešení bezpečně ukládá citlivá data včetně šifrování hesel pomocí AES 256.	WPP bezpečně ukládá citlivá data a šifruje hesla pomocí AES-256.	zde
	SSH klíče	Řešení bezpečně spravuje a distribuuje SSH klíče.	WPP bezpečně spravuje a distribuuje SSH klíče.	zde
	Rotace hesel a klíčů	Řešení umožňuje automaticky měnit hesla a SSH klíče pro specifické systémy či skupiny účtů.	WPP umožňuje automatickou změnu hesel a SSH klíčů pro specifické systémy nebo skupiny účtů.	zde
	Výjimky v rotaci	Řešení umožňuje definovat výjimky pro	WPP umožňuje definovat	zde

	hesel	zamezení automatických rotací hesel a SSH klíčů u určitých účtů.	výjimky, které zabrání automatické rotaci hesel a SSH klíčů u specifických účtů.	
	Časové intervaly rotace hesel	Řešení umožňuje definovat časové intervaly pro provádění automatizovaných změn hesel a SSH klíčů.	WPP umožňuje nastavit časové intervaly pro automatickou změnu hesel a SSH klíčů.	zde
	Rotace hesel po každé relaci	Řešení umožňuje iniciovat změnu hesel a SSH klíčů po každém odhlášení.	WPP umožňuje automatickou změnu hesel a SSH klíčů po každém odhlášení uživatele.	zde
	Komplexita generovaných hesel	Řešení umožňuje definovat komplexitu generovaných hesel dle počtu znaků, využití malých / velkých písmen a speciálních znaků.	WPP umožňuje nastavit komplexitu generovaných hesel, včetně počtu znaků, použití malých a velkých písmen a speciálních znaků.	zde
	Rest API	Řešení musí umožňovat změnu hesel pomocí REST API.	WPP podporuje změnu hesel pomocí REST API.	zde
	Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace, např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat	WPP zprostředkovává správcovský přístup na cílový systém pomocí jump serveru, který využívá zvolený komunikační protokol, aplikaci a příslušný privilegovaný účet. Izolace přístupu je možná až na úroveň aplikace, což zajišťuje, že uživatel nemá přístup k přihlašovacím údajům. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení lze navázat přes GUI řešení nebo pomocí standardních protokolů RDP a SSH. Všechny možnosti připojení podporují silnou autentizaci.	zde

		jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, RADIUS nebo SAML).		
	Autentizace privilegovaných uživatelů	Řešení poskytuje různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně: 1. Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na PIM/PAM řešení. 2. Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů (např. root, admin, privilegovaný lokální účet). 3. Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.	WPP poskytuje různé metody autentizace privilegovaných uživatelů, včetně autentizace pomocí stejných přihlašovacích údajů jako pro PIM/PAM řešení, statických a bezpečně uložených přihlašovacích údajů a vyzváním uživatele k opětovnému zadání přihlašovacích údajů bez jejich zaznamenání.	zde
	Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě.	WPP umožňuje bezpečné připojení na vybrané webové aplikace, přístup do cloudu a	zde

		PIM/PAM řešení zprostředkuje přihlášení do koncové webové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.	sociálních sítí. Přihlášení do koncové webové aplikace je zprostředkováno pomocí silného privilegovaného účtu, což umožňuje transparentní SSO bez nutnosti znát hesla.	
	Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat - minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací klik na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.	WPP umožňuje monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání. Záznam relace je vytvářen kontinuálně a umožňuje zpětné vyhledávání ve formě metadat. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran a je dostupné z GUI řešení.	zde
	Možnosti nahrávání relací	Řešení umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin.	WPP umožňuje aktivaci nebo deaktivaci nahrávání relací podle jednotlivých uživatelských skupin.	zde
	Terminace relací	Řešení nabízí možnost automatické terminace potenciálně nebezpečných relací na základě definovaných procesů, příkazů nebo aplikací, které uživatel spouští na spravovaném systému. Nastavení je možné provádět pro	WPP umožňuje automatickou terminaci potenciálně nebezpečných relací na základě definovaných procesů, příkazů nebo	zde

		různé uživatele nebo uživatelské skupiny.	aplikací. Nastavení lze provádět pro různé uživatele nebo uživatelské skupiny.	
	Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci.	WPP umožňuje sledování aktivních relací dalším uživatelem, například auditorem, a v případě potřeby ukončení sledované relace.	zde
	Časové rámce relací	Řešení umožňuje vyžadování schválení relace v určitých časových rámcích - Např. pondělí-pátek, 6:00-18:00 bez potřeby schválení, v jiných časech pouze po schválení.	WPP umožňuje nastavit časové rámce pro relace, kde je vyžadováno schválení, například pondělí-pátek od 6:00 do 18:00 bez potřeby schválení, v jiných časech pouze po schválení.	zde
	Blokace procesů	Řešení umožňuje blokování vybraných procesů na systémech Windows.	WPP umožňuje blokování specifických procesů na systémech Windows.	zde
	Schvalování relací	Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu: 1. Privilegovaný uživatel požádá o přístup. 2. Definovaní uživatelé obdrží žádost o schválení přístupu. 3. Minimální definovaný počet uživatelů schválí žádost. 4. Privilegovaný uživatel po schvalovacím procesu automaticky	WPP umožňuje schvalování přístupu privilegovaného uživatele k monitorovaným systémům. Proces schvalování zahrnuje žádost o přístup, schválení definovanými uživateli a automatické získání přístupu po schválení.	zde

		získá přístup k monitorovanému systému.		
	Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.	WPP umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.	zde
	Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.	WPP umožňuje audit jednotlivých akcí uživatelů s privilegovanými účty, včetně zobrazení hesla, změn uložených údajů a vytvoření relace.	zde
	Audit administrátorských akcí	Řešení musí umožňovat zobrazení veškerých aktivit administrátora řešení.	WPP umožňuje zobrazení všech aktivit administrátora řešení.	zde
	Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.	WPP umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.	zde
	Export auditních dat	Systém musí umožňovat export auditních záznamů.	WPP umožňuje export auditních záznamů.	zde
	Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.	WPP zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, včetně možností reportování a textových logů.	zde
	Zabezpečení auditních záznamů	Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.	WPP ukládá auditní záznamy bezpečně v zašifrované podobě, přístup k nim má pouze oprávněný uživatel.	zde
	Monitoring pomocí Rest API	Systém umožňuje monitoring jednotlivých komponent pomocí Rest API - integrace s monitoring systémy zadavatele.	WPP umožňuje monitoring jednotlivých komponent pomocí Rest API a integraci s monitoring systémy zadavatele.	zde
	Podpora systémů	Řešení musí umožňovat správu pro různé	WPP podporuje správu různých druhů koncových systémů, včetně	zde

	zadavatele	druhy koncových systémů – minimálně: • Windows 10,11 Windows Server, 2012, 2016, 2019, 2022, 2025 • Linux Red Hat, Suse, Debian, Centos, Unix, AIX • Active Directory • Virtualizační platformy VMWare, Hyper-V • Databáze MS SQL, Oracle, MySQL (MariaDB) • Zařízení Sophos, Extreme Networks	Windows 10, 11, Windows Server 2012, 2016, 2019, 2022, 2025, Linux Red Hat, Suse, Debian, Centos, Unix, AIX, Active Directory, virtualizačních platforem VMWare, Hyper-V, databází MS SQL, Oracle, MySQL (MariaDB) a zařízení Sophos, Extreme Networks.	
	Podpora přihlášení bez nutnosti manuálně vkládat heslo a nahrávání relací pro následující aplikace a protokoly	protokoly: RDP, SSH, Telnet DB klienti: SQL Management Studio Web GUI: MS Edge, Chrome, Firefox	WPP podporuje přihlášení bez nutnosti manuálně vkládat heslo a nahrávání relací pro protokoly RDP, SSH, Telnet, DB klienty SQL Management Studio a webové GUI MS Edge, Chrome, Firefox.	zde
	MFA – multi factor autentizace	Řešení musí buď nativně nebo integrací nástroje třetí strany, vynucovat multi factor autentizaci. Minimálně na úrovní LDAP/S, RADIUS, SAML. MFA je vyžadována jako nedílná komponenta požadovaného řešení.	WPP nativně nebo integrací nástroje třetí strany vynucuje multi-factor autentizaci (MFA) na úrovni LDAP/S, RADIUS, SAML. MFA je nedílnou součástí řešení.	zde
	SIEM integrace	Řešení musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog.	WPP umožňuje integraci s nástroji SIEM pro přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog.	zde

	Architektura řešení	Řešení je dodáváno jako virtuální software appliance (obsahuje i OS) s podporou pro virtuální prostředí Hyper-V/VMWARE.	WPP je dodáván jako virtuální software appliance, který obsahuje i operační systém a podporuje virtuální prostředí Hyper-V a VMware.	zde
	Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení s hardeningem zajištěným výrobcem řešení. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.	WPP splňuje vysoké nároky na zabezpečení s hardeningem zajištěným výrobcem. Úložiště dat je vysoce zabezpečeno a databáze dat je součástí řešení, což eliminuje potřebu nástrojů třetích stran. Tento požadavek platí pro veškerá data včetně HA a DR.	zde
	Vyhledávání systémů	Řešení umožňuje vyhledávání systémů a privilegovaných účtů formou skenování RDP + SSH portů a importů z AD.	WPP umožňuje vyhledávání systémů a privilegovaných účtů pomocí skenování RDP a SSH portů a importů z Active Directory.	zde
	Onboarding systémů	Řešení disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů.	WPP nabízí mechanismus pro plnou nebo částečnou automatizaci onboardingu nově nalezených zařízení a účtů.	zde
	Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované.	WPP umožňuje bezpečné zálohování dat systému, přičemž zálohy jsou šifrované.	zde
	Úložiště	Řešení umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.	WPP umožňuje ukládání zaznamenaných relací lokálně nebo na externí úložiště CIFS/NFS.	zde

	Druh licence	Licence musí být perpetuální s roční podporou. Licence není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů.	WPP nabízí perpetuální licenci s roční podporou, která není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů.	zde
	Licence počet zařízení	Licence je pro minimálně pro 10/50 privilegovaných uživatelů (interních/externích) a 200 spravovaných zařízení a aplikací	WPP licence pokrývá 200 spravovaných zařízení a aplikací. Počet privilegovaných uživatelů se nerozlišuje.	Součástí nabídky
	Podpora řešení	Dodávka musí obsahovat podporu výrobce (maintenance) na období min. 60 měsíců. Technická podpora musí být minimálně v rozsahu 8x5.	WPP zahrnuje podporu výrobce (maintenance) na období 60 měsíců a tech. podporu v rozsahu 8x5.	Součástí nabídky

Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management, SIEM)

Část	**Parametr**	**Popis povinného parametru**	**Popis způsob naplnění tohoto povinného parametru včetně uvedení značkové specifikace**	**Odkaz na část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu logů	Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware.	Logmanager poskytuje centralizovanou platformu pro sběr, zpracování a analýzu logů z různých zdrojů, včetně aplikací, operačních systémů a síťových zařízení. Podporuje různé formáty logů a protokoly pro zajištění kompatibility a	zde

			efektivního zpracování dat.	
	Architektura	Virtuální appliance, samostatně funkční nezávisle na infrastruktuře zadavatele.	Logmanager je dostupný jako virtuální appliance, který může být nasazen na různých virtualizačních platformách, jako jsou VMware a Hyper-V. Tento přístup umožňuje flexibilní nasazení a škálovatelnost bez závislosti na specifické infrastruktuře.	zde
	Typ licence	Perpetuální, licence není omezena počtem zařízení/systémů zasílající logy.	Perpetuální licence Logmanageru umožňuje neomezený počet zařízení a systémů pro zasílání logů, což poskytuje flexibilitu a škálovatelnost pro různé velikosti a typy organizací.	zde
	Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.	Logmanager nabízí intuitivní grafické uživatelské rozhraní, které umožňuje administrátorům a operátorům snadno spravovat systém, provádět úvodní nastavení a monitorovat logy a události v reálném čase.	zde
	Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.	Logmanager podporuje autentizaci uživatelů prostřednictvím Active Directory nebo LDAP, což zajišťuje bezpečný přístup k	zde

			systému. V případě výpadku těchto služeb je k dispozici záložní autentizace z lokální databáze.	
	Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému.	Systém umožňuje definovat různé uživatelské role s konkrétními přístupovými právy, což zajišťuje bezpečné a efektivní řízení přístupu k uloženým logům a ovládacím prvkům systému.	zde
	Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows.	Logmanager umožňuje bezagentový sběr logů z různých systémů, s výjimkou Windows, kde je vyžadován agent pro sběr dat. Tento přístup minimalizuje potřebu instalace a údržby agentů na většině zařízení.	zde
	Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text a textový popis události shodný s Windows Event Viewerem.	Windows agent Logmanageru umožňuje kompletní správu a aktualizaci prostřednictvím administrátorské konzole. Zajišťuje sběr dat z textových a Event logů, šifrovanou komunikaci, buffer pro případ ztráty komunikace a překlad kódů na text, což usnadňuje analýzu událostí.	zde
	Protokoly	Příjem a zpracování logů, událostí a další strojově generovaných dat minimálně protokoly UDP/TCP	Logmanager podporuje příjem a zpracování logů a událostí	zde

		514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).	prostřednictvím různých protokolů, včetně UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně), což zajišťuje širokou kompatibilitu a bezpečnost přenosu dat.	
	Formáty logů	Minimálně RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog.	Logmanager podporuje různé formáty logů, včetně RAW, Syslog, CEF, LEEF, JSON RFC7159 a Windows EventLog, což umožňuje flexibilní zpracování a analýzu dat z různých zdrojů.	zde
	Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.	Logmanager umožňuje příjem logů na alespoň 50 UDP a TCP portech, což usnadňuje třídění a organizaci vstupních zpráv pro efektivní zpracování a analýzu.	zde
	Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy.	Logmanager poskytuje integrované nástroje pro parsování a normalizaci přijatých logů a událostí, což eliminuje potřebu externích aplikací a zajišťuje efektivní zpracování dat.	zde
	Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.	Logmanager zajišťuje ochranu uložených logů proti mazání nebo modifikaci a každý log je opatřen unikátním identifikátorem pro	zde

			jednoznačnou identifikaci, což zvyšuje bezpečnost a integritu dat.	
	Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrovaná podpora zobrazení TOP X událostí za zvolené časové období.	Logmanager nabízí pokročilé grafické vizualizační nástroje, které umožňují dynamickou vizualizaci logů a událostí. Změnou filtru v jednom grafu se automaticky upraví ostatní grafy, což usnadňuje analýzu dat. Podporuje také zobrazení TOP X událostí za zvolené časové období.	zde
	Pracovní plochy	Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání.	Logmanager poskytuje předpřipravené dashboardy, které umožňují rychlý přístup k uloženým datům podle kategorií zdrojových zařízení a logického členění. Tyto pohledy jsou průběžně aktualizovány výrobcem a systém také podporuje tvorbu a ukládání vlastních uživatelských dashboardů.	zde
	Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min. 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti.	Logmanager zajišťuje ochranu proti ztrátě logů při přetížení systému tím, že ukládá nezpracované logy do vyrovnávací paměti s kapacitou minimálně 25 GB. Systém také notifikace správce při riziku	zde

			zaplnění této paměti, což zajišťuje kontinuitu sběru dat.	
	Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.	Logmanager umožňuje doplňování logů o další údaje, jako je umístění zařízení, typ zařízení a jeho kritičnost. Tato funkce zajišťuje detailnější a kontextově bohatší analýzu logů, což usnadňuje správu a monitorování různých zdrojů dat.	zde
	Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova.	Logmanager poskytuje integrovanou archivaci logů, která zajišťuje jejich dlouhodobé uchování a integritu. Systém také podporuje obnovu archivovaných logů, což umožňuje přístup k historickým datům pro analýzu a audit.	zde
	Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy.	Logmanager automaticky doplňuje reverzní DNS záznamy k IP adresám a identifikuje výrobce zařízení podle MAC adresy. Tato funkce zjednodušuje správu sítě a zvyšuje přesnost identifikace zařízení v síti.	zde
	Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu,	Logmanager podporuje přidávání doplňkových časových	zde

		slouží jako výchozí časový údaj pro systém.	razítek k zaznamenaným událostem a logům. Tato razítka slouží jako výchozí časový údaj pro systém, což zajišťuje přesné časové řazení a analýzu událostí.	
	Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalostí (např. SQL dotazů apod.) napříč všemi typy data a zařízení.	Logmanager umožňuje snadné multikriteriální vyhledávání událostí napříč všemi typy dat a zařízení bez nutnosti speciálních znalostí, jako jsou SQL dotazy. Tento nástroj usnadňuje rychlé a efektivní vyhledávání relevantních informací.	zde
	Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování).	Logmanager podporuje rychlé vyhledávání i v aktuálně uložených položkách díky průběžnému indexování dat. Tato funkce zajišťuje okamžitý přístup k nejnovějším informacím a událostem.	zde
	Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran.	Logmanager automaticky doplňuje geolokační informace k událostem a zobrazuje je graficky na mapě. Tato funkce nevyžaduje služby třetích stran, což zajišťuje bezpečnost a integritu dat.	zde
	Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností	Logmanager nabízí integrovaný reportovací nástroj, který	zde

		vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem.	obsahuje přednastavené reporty a umožňuje uživatelům vytvářet a upravovat vlastní reporty bez potřeby speciálních znalostí. Přednastavené reporty jsou průběžně aktualizovány výrobcem, což zajišťuje aktuálnost a relevanci informací.	
	Integrace	Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů.	Logmanager poskytuje integrované REST API rozhraní, které umožňuje autorizovaný přístup ke strukturované databázi logů. Tato funkce usnadňuje integraci s dalšími systémy a automatizaci procesů.	zde
	Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb.	Logmanager obsahuje grafický nástroj pro tvorbu vlastních parserů logů, který umožňuje testování a ladění parserů s okamžitým zobrazením výsledků a identifikací chyb. Tento nástroj zjednodušuje přizpůsobení systému specifickým potřebám uživatele.	zde
	Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Hyper-V, Windows (vč. DNS, DHCP), Icewarp, MS SQL, Sophos, HPE/Aruba, Dell servery, Synology, Linux,	Logmanager podporuje širokou škálu konektorů pro různé technologie, včetně Active Directory, Hyper-V, Windows	zde

		Apache, Extreme Networks, MikroTik	(včetně DNS a DHCP), Icewarp, MS SQL, Sophos, HPE/Aruba, Dell servery, Synology, Linux, Apache, Extreme Networks a MikroTik. Tyto konektory zajišťují kompatibilitu a snadnou integraci s různými systémy.	
	Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP.	Logmanager obsahuje předpřipravené alerty a grafický nástroj pro tvorbu vlastních notifikací a alertů. Tyto alerty mohou být generovány na základě definovaných podmínek v přijatých datech a odesílány prostřednictvím SMTP, Syslog nebo TCP.	zde
	Výkon	Min. 5000 EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému 200%.	Logmanager je navržen tak, aby zvládl minimálně 5000 událostí za sekundu (EPS) a krátkodobě (minimálně 10 minut) přetížení až na 200 % kapacity. Tento výkon zajišťuje spolehlivý sběr a zpracování velkého množství dat v reálném čase.	zde
	Úložiště logů	Logy musí být ukládány do databáze neomezené velikostí (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.	Logmanager ukládá logy do databáze bez omezení velikosti, přičemž příslušná licence je součástí dodávky. Systém podporuje kompresi ukládaných dat, což optimalizuje využití úložiště a zajišťuje efektivní	zde

			správu velkých objemů logů.	
	Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje).	Server je vybaven redundantním napájením s minimálně dvěma nezávislými zdroji, což zajišťuje nepřetržitý provoz a minimalizuje riziko výpadků způsobených selháním napájení.	Viz nabídka serverů
	Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade.	Logmanager podporuje integrované aktualizace systému prostřednictvím administrátorské konzole, včetně možnosti downgrade. Tato funkce zajišťuje, že systém je vždy aktuální a může být snadno spravován a udržován.	zde
	Zálohování	Integrované zálohování a obnova konfigurace.	Logmanager poskytuje integrované nástroje pro zálohování a obnovu konfigurace, což zajišťuje ochranu dat a rychlou obnovu systému v případě potřeby.	zde
	Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden.	Logmanager je škálovatelný a může být propojen s dalšími systémy stejného výrobce. Toto propojení zvyšuje kapacitu, výkon (včetně vyhledávání) a dostupnost, přičemž propojené systémy se navenek chovají jako jeden celek.	zde

	Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce.	Logmanager poskytuje plnohodnotnou dokumentaci v českém jazyce, která je shodná s originální dokumentací. Tato dokumentace usnadňuje uživatelům správu a konfiguraci systému.	zde
	Záruka	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace.	Systém obsahuje záruku 60 měsíců. Virtualizační platforma zahrnuje opravu hardware do druhého pracovního dne v místě instalace a nárok na nové verze firmware/software a aktualizace. Tato záruka zajišťuje dlouhodobou podporu a spolehlivost systému.	V ceně nabídky
SIEM	Základní funkce	Řešení musí celkově pokrývat tyto funkce: Log management, Event Management, pokročilou korelaci z více zdrojů, příjem a sběr logů, centrální správu a reporting, a to včetně vlastních logů.	Nabízené řešení Wazuh umožňuje, log management, Event management, pokročilou korelaci napříč zdoji, příjem a sběr logů, centrální webovou konzoli, reporting, včetně auditu	zde
	Řešení musí zajistit	Identifikaci hrozeb se známými projevy chování a jejich začlenění do korelačních pravidel. Identifikaci a predikci hrozeb s neznámými projevy chování na základě anomálií v provozu. Napojení řešení na světovou threat inteligenční bázi a využití inovativních technik umělé inteligence a strojového učení. Pomocí nově vydaných IoC (Indicator of Compromise) zpětně	Nabízené řešení Wazuh umožňuje vytváření CDB listů, sytém dokáže ověřit, zda se pole extrahované během fáze dekódování nachází v seznamu CDB. Hlavním využitím této funkce je vytvoření seznamu povolených nebo zakázaných	zde

		vyhledávat a detekovat hrozby (zejména IP adresy, Doménová jména, URL adresy, Hash hodnoty, Emailové adresy, Souborové cesty, Porty a protokoly, Chování, vzory a behaviorální znaky, Certifikáty, Tokeny a autentizační informace, Síťové logy) v sesbíraných log záznamech.	uživatelů, hashů souborů, IP adres, doménových jmen a další. Systém dokáže detekuje škodlivé soubory prostřednictvím integrace s VirusTotal, výkonnou platformou, která agreguje více antivirových produktů a online skenovací engine. Kombinace tohoto nástroje s naším modulem FIM poskytuje efektivní způsob inspekce monitorovaných souborů na přítomnost škodlivého obsahu. Analýza chování, strojové učení je řešena za pomocí modulu anomaly detection. Všechny požadované funkce jsou rozšířené díky vlastnímu vývoji zadavatele.	
	Podporované protokoly	Syslog, Windows Events Collection (WinRM/RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol. Bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém).	Podporované všechny sběry logů za pomocí nativního napojení do nabízeného systému + díky vlastnímu vývoji, propojovacích mechanizmů.	zde
	Kompatibilita	Systém musí být kompatibilní s nabízeným systémem pro správu logů.	Systém umožňuje integraci	zde
	Licence	Licence pro trvalé zpracování 5 000 EPS nebo ekvivalentu 200 GB denně při průměrné velikosti zdrojové události 600 B s možností rozšíření. Systém musí umožňovat krátkodobé překročení	Řešení Wazuh není v tomto směru licenčně omezeno, kapacity budou dosažený sizingem HW.	zde

		EPS a možnost ukládat nezpracované logy. Součástí řešení bude licence pro skener zranitelností pro minimálně 1500 IP adres. Licence pro neomezený počet zdrojů událostí připojený do SIEM. Řešení nebude licenčně omezovat úložnou kapacitou nebo dobu uložení. Licence umožňuje dočasné trojnásobné překročení limitu příjmu událostí bez ztráty jejich korelace. Řešení nebude licenčně omezeno počtem používaných korelačních pravidel. Řešení nebude licenčně omezeno počtem generovaných reportů. Řešení nebude licenčně omezeno počtem současně připojených administrátorů či operátorů.		
	Skener zranitelností	Dodané řešení musí obsahovat skener zranitelnosti. Součástí skeneru zranitelností bude funkcionalita schopná provádět pravidelnou, automatickou detekci zranitelností minimálně na základě volně dostupných databází (jako jsou Red Hat, Microsoft a National Vulnerability Database (NVD)), v lepším případě bude skener přímo doplněn o další vlastní nebo placené databáze. Systém musí být schopen využít detekované anomálie a zdroje informací pro korelaci s logy do jednotných incidentů.	Požadavek bude naplněn pomocí kombinace technologií Wazuh a OpenVAS. OpenVAS bude nasazen jako skener zranitelností, schopný provádět pravidelnou a automatickou detekci zranitelností na základě volně dostupných databází, jako jsou Red Hat, Microsoft, a National Vulnerability Database (NVD). Wazuh pak zajistí korelaci detekovaných zranitelností a anomálií s logy z různých systémů, což povede ke sjednocení těchto informací do jednotných incidentů. Tím bude dosaženo požadované	zde

			funkčnosti řešení.	
	Management	Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní. Rozhraní nesmí vyžadovat instalaci dalšího SW na straně uživatelů technologie Java, Flash, apod. a nesmí vyžadovat používání nebo instalaci tlustého klienta. Řešení musí umožňovat definici uživatelských oprávnění pro možnost oddělení přístupu jednotlivých administrátorů k jednotlivým zdrojům logů a toků, jejich skupinám či síťovým segmentům. Přístup je možné řídit na základě členství ve skupinách Active Directory.	Požadavek bude naplněn pomocí kombinace technologií Wazuh, OpenSearch a vlastního vývoje zadavatele. Wazuh poskytne centralizovanou správu všech komponent a administrativních funkcí ve webovém uživatelském rozhraní, které nevyžaduje instalaci dalšího softwaru, jako jsou Java, Flash, nebo tlustý klient. Veškerá správa bude probíhat přímo v rozhraní založeném na moderních webových technologiích. Řešení umožní definovat uživatelská oprávnění pro oddělení přístupů jednotlivých administrátorů k různým zdrojům logů, tokům, jejich skupinám či síťovým segmentům. Navíc bude přístup řízen na základě členství ve skupinách Active Directory, což zajistí efektivní a bezpečné řízení přístupu k systémovým zdrojům.	zde
	Šifrování	Komunikace mezi zdroji logů a SIEM je šifrovaná dle možností zdrojů logů.	Požadavek na šifrovanou komunikaci mezi zdroji logů a SIEM bude naplněn pomocí	zde

			technologie Wazuh. Veškerá komunikace mezi Wazuh agenty, síťovými prvky, a samotným Wazuh serverem může být šifrována například pomocí TLS (Transport Layer Security), což zajistí bezpečný přenos dat. Wazuh podporuje širokou škálu zdrojů logů, včetně Syslogu a síťových zařízení, a v případech, kdy tyto zdroje podporují šifrovanou komunikaci, může být tato možnost plně využita.	
	Integrace	Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů. Systém ale musí rovněž umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti externích autentizačních mechanismů).	Požadavek na integraci s adresářovým systémem (LDAP, Active Directory) pro autentizaci uživatelů bude naplněn prostřednictvím technologie Wazuh, OpenSearch a vlastního vývoje zadavatele. Wazuh umožní integraci s LDAP a Active Directory, což zajistí centralizovanou autentizaci uživatelů a jejich správu na základě adresářového systému organizace. Současně bude systém podporovat také lokální účty, které umožní přihlašování v případě, že externí autentizační mechanismy, jako	zde

			LDAP nebo Active Directory, nejsou dostupné.	
	Automatizace	Automatické připojení a samoučící rozpoznání připojených zařízení.	Wazuh umožňuje automatické připojení nainstalovaného agenta, automatický sběr logů, kdy není nutné definovat zdroj. Systém automaticky, u podporovaných systému, logy zařadí do správné kategorie.	zde
	Aktualizace	Řešení musí umožňovat automatické aktualizace od výrobce. Zejména se jedná o aktualizaci knihoven zařízení a zdrojů logů. Tato funkcionalita bude součástí produktové podpory výrobce.	Automatická aktualizace je řešena za pomocí vlastního vývoje zadavatele, vytvořením automatizovaného skriptu.	zde
	Parserování	Systém umožňuje dopsání parseru pro libovolné zařízení, musí být schopný zpracovat i logy mimo přednastavenou knihovnu. Dokumentace musí obsahovat přehledný návod na vytváření parserů.	Požadavek na automatické aktualizace od výrobce bude naplněn prostřednictvím technologie Wazuh. Wazuh poskytuje integrovaný mechanismus, který umožňuje automatickou aktualizaci knihoven zařízení a zdrojů logů. Systém pravidelně stahuje aktualizace od výrobce, včetně nových verzí pravidel, signatur a detekčních knihoven, což zajistí aktuální a efektivní detekci hrozeb. Tyto aktualizace jsou automaticky aplikovány bez nutnosti manuálního zásahu, a jsou součástí produktové	zde

			podpory poskytované výrobcem Wazuh.	
	Analýza chování uživatelů	Vestavěný modul výrobce pro Analýzu chování uživatelů na základě mechanismů strojového učení.	Řešeno za pomocí OpenSearch a funkce Anomaly Detection	zde
	Zálohování	Poskytování automatického backup/recovery procesu.	Řešeno za pomocí vlastního vývoje zadavatele. Vlastní skript pro naplnění tohoto požadavku.	zde
	Analytika	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box).	Požadavek na poskytování analytických a korelačních funkcí bez dalších zásahů a činností bude naplněn prostřednictvím technologie Wazuh. Wazuh nabízí out-of-the-box řešení, které poskytuje předdefinované analytické a korelační funkce okamžitě po instalaci. Systém je vybaven vestavěnými pravidly pro detekci hrozeb, automatickou analýzu logů a korelaci dat z různých zdrojů, aniž by bylo nutné provádět dodatečné konfigurace.	zde
	Retenční politiky	Možnost nastavení více filtrů retenčních politik pro různé zdroje dat.	Požadavek na možnost nastavení více filtrů retenčních politik pro různé zdroje dat bude naplněn prostřednictvím technologie Wazuh,	zde

			OpenSearch a vlastního vývoje zadavatele. Wazuh umožňuje vytváření různých indexů pro různé zdroje dat, což umožňuje aplikovat specifické retenční politiky pro každý zdroj logů	
	Alerting	Požadujeme automatické vytváření souhrnných informací o bezpečnostních hrozbách na základě korelace dílčích událostí. Řešení musí poskytnout alerting: • vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení • při porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice • při výpadku logů z konkrétního zařízení.	Požadavek na automatické vytváření souhrnných informací o bezpečnostních hrozbách na základě korelace dílčích událostí bude naplněn pomocí technologie Wazuh a vlastního vývoje zadavatele. Wazuh umožňuje automatickou korelaci dílčích událostí z monitorovaných zařízení, což vede k vytváření souhrnných informací o detekovaných bezpečnostních hrozbách.	zde
	Workflow	Požadujeme zpracování a vyhodnocení identifikovaných hrozeb formou jednoduchého workflow.	Požadavek na zpracování a vyhodnocení identifikovaných hrozeb formou jednoduchého workflow bude naplněn prostřednictvím technologie Wazuh a vlastního vývoje zadavatele, která automaticky detekuje a klasifikuje hrozby na základě logů z monitorovaných systémů, následně je automatizovaně zpracuje podle předem definovaného	zde

			workflow, přičemž umožňuje zasílání alertů konkrétním týmům nebo administrátorům pro další kroky, jako je analýza nebo eskalace incidentu, a nakonec poskytuje reporty pro vyhodnocení a sledování průběhu řešení hrozeb	
	Vykonávání akcí	Vykonávání akcí v závislosti na přijatém logu jako např. zaslat e-mail, notifikaci nebo spustit předem definovaný skript.	Požadavek na vykonávání akcí v závislosti na přijatém logu bude naplněn prostřednictvím technologie Wazuh a vlastního vývoje zadavatele, která umožňuje automatické provádění akcí, jako je zaslání e-mailu, odeslání notifikace nebo spuštění předem definovaného skriptu, na základě předdefinovaných pravidel a detekovaných událostí v přijatých logech.	zde
	Geolokace	Schopnost pracovat s IP geolokacemi (botnet kanály atp.).	Požadavek na schopnost pracovat s IP geolokacemi bude naplněn prostřednictvím technologie Wazuh a vlastního vývoje zadavatele, která umožňuje integraci s databázemi IP geolokací pro analýzu a sledování geografického původu síťového provozu.	zde

	Klasifikace událostí	Vestavěný mechanismus na klasifikaci systémů podle typu (např. e-mail server vs. databázový server).	Bude naplněno pomocí technologie Wazuh a vytváření Tagu pro konkrétní typy systému	zde
	Reporting	Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy. Požadujeme pravidelnou, plánovanou tvorbu vydefinovaných reportů minimálně ve formátech PDF a CSV. Nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS.	Požadavek na poskytování rozhraní pro reporting bude naplněn prostřednictvím technologie Wazuh a její integrace, OpenSearch Dashboards a vlastního vývoje zadavatele, která umožňuje vytváření nových sestav bez nutnosti psaní SQL dotazů. Toto rozhraní poskytuje uživatelsky přívětivou platformu, ve které mohou administrátoři snadno sestavovat a přizpůsobovat reporty podle potřeb organizace.	zde
	Konsolidace výsledků	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.	Požadavek na konsolidaci výsledků z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů, bude naplněn prostřednictvím technologie Wazuh. Wazuh je navržen tak, aby integroval data z různých nástrojů, jako jsou vulnerability scannery (např. OpenVAS), risk management	zde

			nástroje a externí bezpečnostní informační zdroje, čímž umožňuje centralizovanou správu bezpečnostních informací.	

Nástroje pro zajišťování úrovně dostupnosti informací – HW pro zajištění provozu implementovaných řešení

Část	**Parametr**	**Popis povinného parametru**	**Popis způsob naplnění tohoto povinného parametru včetně uvedení značkové specifikace**	**Odkaz na část nabídky, kde je možné ověřit naplnění parametru**
Server (hypervizor) SDS – 2ks	Identifikace nabízeného řešení	Jednoznačná identifikace serveru (název, typ, označení výrobce apod.)	Dell PowerEdge R760xs	Poweredge-r760xs.pdf
	Provedení	Umístitelné do racku, včetně montážního materiálu, max. 2U. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Zásuvné ližiny s managementem kabeláže. Uzamykatelný čelní panel s LCD displejem s možností zobrazení standardní stavové informace na čelním panelu s výraznou indikací nestandardních a chybových stavů či parametrů (min. napájení, teplota, vada disku) v textové formě.	Server má standardní 2U rozměry, včetně montážního materiálu s managementem kabeláže, barevně označené hot-plug komponenty, pro přístup ke všem komponentám není nutné nářadí. Server je doplněn o uzamykatelný čelní panel na kterém se nachází LCD display, který zobrazuje nestandardní a chybová hlášení nejen změnou barvy, ale i v textové formě.	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	CPU	Max. 2x CPU, z licenčních důvodů max. 16 jader. Výkon serveru dle SPECrate®2017: SPECrate®2017_int_base min. 177 bodů, SPECrate®2017_fp_base min. 250 bodů	2x procesor, Intel® Xeon® Gold 5415+ 2.9G, 8C/16T, 16GT/s, 22.5M Cache, Turbo, HT (150W) DDR5-4400. SPECrate®2017_int_base min. 177 bodů SPECrate®2017_fp_base min. 229 bodů	http://www.spec.org
	RAM	Min. 16 slotů pro DDR5 RDIMM. Min. 256 GB RAM ECC, min. 4800 MT/s. Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s	Server obsahuje 16 slotů pro DDR5 je osazen 4x 64GB RDIMM, 4800MT/s Dual Rank osazení je optimální pro výkon s CPU.	Poweredge-r760xs-technical-guide.pdf

		CPU.		
	Diskový subsystém	Šasi serveru musí pojmout min. 12 disků formátu 3.5", přístupných v hot-swap rámečcích z přední strany serveru. HW řadič RAID, úrovně HW RAID 0, 1, 5, 6, 10. Rozhraní disků: SAS/SATA. Osazení: 2x 3.84 TB SSD Mixed Used, 4x 20TB SAS	Šasi serveru je 3.5" Chassis with up to 12 Hard Drives (SAS/SATA). Server je osazen 4x 20TB Hard Drive SAS 12Gbps 7.2K 512e 3.5in Hot-Plug, AG Drive a 2x 3.84TB SSD vSAS Mixed Use 12Gbps 512e 2.5in w/3.5in HYB CARR ,AG Drive SED, 3DWPD	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Spouštěcí jednotka (Boot Drive)	Musí být zajištěna dvojicí SSD disků v RAID1 s kapacitou min. 960 GB. Disky musí být připojeny na samostatný RAID řadič mimo Diskový subsystém. Disky nesmí zabírat pozici v 16 diskovém šasi vyhrazeném pro Diskový subsystém. Disky musí být hot-swap, přístupné z přední nebo zadní strany serveru.	Server je osazen BOSS-N1 controller card + with 2 SED M.2 960GB (RAID 1). Disky jsou hot-plug a přístupné ze zadní strany serveru. Disky nezabírají pozice určené pro data.	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Porty	Min. 3x externí USB, z toho min. 1x USB 3.0. Min. 1x dedikovaný USB management port. Min. 2x VGA port (jeden na přední a jeden na zadní straně serveru).	Server je osazen 3x USB konektory (2x USB 2.0 a 1x USB 3.0) z toho jeden je na čelním panelu s podporou bootování. Server má dedikovaný USB management port. Server má VGA z přední a zadní strany serveru.	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Napájecí zdroje	2x napájecí zdroj max. 1100 W, redundance, min. Platinum energetická účinnost dle certifikace 80 PLUS. 80 PLUS	Server je osazen Dual, Hot-Plug, Power Supply Fault Tolerant Redundant (1+1), 1100W MM (100-240Vac) Titanium, NAF a splňuje energetická účinnost dle certifikace 80 PLUS.	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Rozšiřující sloty	Min. 3x PCIe slot (Gen5 nebo Gen4).	Server má k dispozici 3x16 PCI slot a 1x8 PCI slot	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Síťové porty	Min. 1x 1GbE dedikovaný management port nezabírající PCIe slot. Min. 2x 1GbE nezabírající PCIe slot. Min. 2x 10/25GbE SFP28	Server obsahuje Broadcom 5720 Dual Port 1Gb On-Board LOM (nezabírá PCI-e slot) a dále Broadcom 57414 Dual Port 10/25GbE SFP28 s možností budoucí výměny. Server má dedikovaný management port pro iDrac	Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf
	Kompatibilita	Microsoft Windows Server, Microsoft Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi	Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi Canonical Ubuntu Server LTS	Poweredge-r760xs.pdf

	Management a vzdálená správa	Vzdálená správa serveru, nezávislá na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení e-mailem, vzdáleného připojení (KVM) prostřednictvím dedikovaného LAN management portu s podporou IPv4 a IPv6. Vzdálená správa musí disponovat vlastním GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných Java nebo ActiveX komponent. Vzdálená správa musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení virtuálních medií (ISO souborů) a možnost vzdáleného připojení USB disku. Management serveru musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro obnovu či přeinstalaci vadného firmware. Management serveru musí z důvodu bezpečnosti umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů. Změna stavu USB portu musí být možná bez nutnosti restartu serveru.	Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi v kombinaci s centrálním managementem Dell OpenManage Server obsahuje iDrac v edici umožňující zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu je možná bez nutnosti restartu serveru.	Poweredge-r760xs-technical-guide.pdf iDrac9-User-Guide.pdf Dell-Openmanage.pdf iDrac9-security-configuration-guide.pdf
	Bezpečnost	Server musí disponovat bezpečnostním systémem ověření komponent. Tento systém musí umožňovat ověřit, že mezi výrobou serveru a doručením k zákazníkovi nebyla konfigurace komponent serveru změněna ani upravena.	Server disponuje Server Secured Component Verification	Poweredge-Secured Component Verification.pdf
	Záruka a technická podpora výrobce	Záruka min. 60 měsíců. Dostupnost podpory 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem	Záruka 60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware. Zařízení umožňuje automatického generování servisního incidentu přímo u	Součástí cenové nabídky https://www.dell.com/support/home/en-us Poweredge-r760xs.pdf Poweredge-r760xs-technical-guide.pdf Dell-SupportAssist.PDF

		hardwaru. Oprava v místě instalace hardwaru. Možnost automatického generování servisního incidentu přímo u výrobce hardwaru (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace softwaru a firmwaru pro komponenty serveru. Podpora prostřednictvím internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmwaru, softwaru a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce), díky záruce ProSupport, dostupnost podpory je 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Dell-prosupport-brochure.PDF
Licence	Operační systém	Licence umožňující provoz virtuálního prostředí a min. 10 virtuálních serverů.	Součástí dodávky serverů je i Windows Server 2022 v edici Datacenter umožňující provoz neomezenoho množství virtuálních serverů stejné edice. Licence je k dispozici pro každý server.	Součástí cenové nabídky
SDS řešení	Provedení	Licence software vysoce dostupného virtualizovaného softwarově definovaného diskového úložiště pro nabízené virtualizační servery.	MS Windows Server 2022 v edici Datacenter, která je součástí dodávky, obsahuje technologii Storage Spaces Direct.	https://learn.microsoft.com/en-us/azure-stack/hci/concepts/storage-spaces-direct-overview
	Replikace	Software musí umožnit minimálně synchronní replikace dat (zrcadlení, mirror, RAID1) mezi uzly SDS (virtualizačními servery).	Technologie Storage Spaces Direct umožňuje synchronní replikaci dat	https://learn.microsoft.com/en-us/azure-stack/hci/concepts/storage-spaces-direct-overview
	Vysoká dostupnost	Automatické překlenutí výpadku jednoho prvků systému – jednoho serveru či jeho komponenty (např. jednoho disku). Včetně podpory zotavení a obnovení.	Řešení disponuje funkcí Failover Clustering, která zajistí překlenutí výpadku jednoho jednoho nebo více nodů. Dále je systém odolný proti jednomu či více disků a podporuje automatické zotavení po obnovení	https://learn.microsoft.com/en-us/azure-stack/hci/concepts/storage-spaces-direct-overview
	Podpora virtualizace	Software bude provozován na úrovni hypervizorů (bude do nich zaintegrován) nabízené serverové	Storage Spaces Direct je integrální součástí nabízených Windows Server 2022 Datacenter	https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison?pivots=windows-server-2025

		virtualizace.		
	Jednotná správa	Správa SDS bude zaintegrována do nástroje pro správu serverové virtualizace pro jednotnou správu.	Storage Spaces Direct je integrální součástí nabízených Windows Server 2022 Datacenter	https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison?pivots=windows-server-2025
	Podpora	Podpora výrobce včetně nároku na nové verze po dobu min 60 měsíců.	Storage Spaces Direct je integrální součástí nabízených Windows Server 2022 Datacenter, podpora končí 14. 10. 2031	https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2022
Mgmt server 1ks	Identifikace nabízeného řešení	Jednoznačná identifikace serveru (název, typ, označení výrobce apod.)	Dell PowerEdge R360	PowerEdge-r360-specsheet.pdf
	Provedení	Umístitelné do racku, včetně montážního materiálu, max. 2U. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Zásuvné ližiny s managementem kabeláže. Uzamykatelný čelní panel.	Server má standardní 2U rozměry, včetně montážního materiálu s managementem kabeláže, barevně označené hot-plug komponenty, pro přístup ke všem komponentám není nutné nářadí. Server je doplněn o uzamykatelný čelní panel	PowerEdge-r360-technical-guide.pdf
	CPU	Max. 1x CPU, z licenčních důvodů max. 16 jader. Výkon serveru dle SPECrate®2017: SPECrate®2017_int_base min. 84 bodů, SPECrate®2017_fp_base min. 99 bodů.	Server je osazen jedním CPU Intel® Xeon® E-2468 2.6G, 8C/16T, 24M Cache, Turbo, HT (65W) DDR5, SPECrate®2017_int_base min. 84,4 bodů, SPECrate®2017_fp_base min. 100 bodů	https://www.spec.org/
	RAM	Min. 4 slotů pro DDR5 RDIMM. Min. 32 GB RAM ECC, min. 4800 MT/s. Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU.	Server je osazen 2x 16GB UDIMM, 5600MT/s ECC, počet paměťových modulů a rozmístění musí je zvoleno pro optimální výkon s CPU.	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	Diskový subsystém	Šasi serveru musí pojmout min. 6 disků formátu 2.5", přístupných v hot-swap rámečcích z přední strany serveru. HW řadič RAID, úrovně HW RAID 0, 1, 5, 6, 10. Rozhraní disků: SAS, SATA (HDD, SSD). Osazení: 2x 1.92 TB SSD HDD Read Intensive“	Šasi serveru je 2.5" Chassis with up to 8 Hard Drives (SAS/SATA) + 2x2.5" Rear SAS/SATA Drives,. Server je osazen 2x 1.92TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug Hard Drive. Server osazen řadičem Front PERC H755 Front Load, úrovně HW RAID 0, 1, 5, 6, 10, cache 8GB	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf Dell-perc11.pdf
	Porty	Min. 3x externí USB, z toho min. 1x USB 3.0. Min. 1x VGA port.	Server je osazen 3x USB konektory (2x USB 2.0 a 1x USB 3.0) z toho jeden je na čelním panelu s podporou bootování. Server má VGA z přední a zadní strany serveru.	

	Napájecí zdroje	Napájecí zdroj max. 1100 W, redundance, min. Platinum energetická účinnost dle certifikace 80 PLUS. 80 PLUS	Server je osazen Dual, Hot-Plug, PSU Fault Tolerant Redundant (1+1), 700W MM HLAC (ONLY FOR 200-240Vac) Titanium	PowerEdge-r360-technical-guide.pdf
	Rozšiřující sloty	Min. 1x PCIe slot (Gen5 nebo Gen4).	Server je osazen 1x PCI slotem	PowerEdge-r360-technical-guide.pdf
	Síťové porty	Min 1x 1GbE dedikovaný management port nezabírající PCIe slot. Min. 2x 1GbE nezabírající PCIe slot.	Server je osazen Broadcom 5720 Dual Port 1Gb On-Board LOM	PowerEdge-r360-technical-guide.pdf
	Kompatibilita	Microsoft Windows Server, Microsoft Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi.	Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi Canonical Ubuntu Server LTS	PowerEdge-r360-specsheet.pdf
	Management a vzdálená správa	Vzdálená správa serveru, nezávislá na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení e-mailem, vzdáleného připojení (KVM) prostřednictvím dedikovaného LAN management portu s podporou IPv4 a IPv6. Vzdálená správa musí disponovat vlastním GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných Java nebo ActiveX komponent. Vzdálená správa musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení virtuálních medií (ISO souborů) a možnost vzdáleného připojení USB disku. Management serveru musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro obnovu či přeinstalaci vadného firmware. Management serveru musí z důvodu bezpečnosti umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů.	Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi v kombinaci s centrálním managementem Dell OpenManage Server obsahuje iDrac v edici umožňující zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu je možná bez nutnosti restartu serveru.	PowerEdge-r360-technical-guide.pdf iDrac9-User-Guide.pdf Dell-Openmanage.pdf iDrac9-security-configuration-guide.pdf

		Změna stavu USB portu musí být možná bez nutnosti restartu serveru.		
	Bezpečnost	Server musí disponovat bezpečnostním systémem ověření komponent. Tento systém musí umožňovat ověřit, že mezi výrobou serveru a doručením k zákazníkovi nebyla konfigurace komponent serveru změněna ani upravena.	Server disponuje Server Secured Component Verification	Poweredge-Secured Component Verification.pdf
	Záruka a technická podpora výrobce	Záruka min. 60 měsíců. Dostupnost podpory 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardwaru. Oprava v místě instalace hardwaru. Možnost automatického generování servisního incidentu přímo u výrobce hardwaru (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace softwaru a firmwaru pro komponenty serveru. Podpora prostřednictvím internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmwaru, softwaru a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Záruka 60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware. Zařízení umožňuje automatického generování servisního incidentu přímo u výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce), díky záruce ProSupport, dostupnost podpory je 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Součástí cenové nabídky https://www.dell.com/support/home/en-us PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf Dell-SupportAssist.PDF Dell-prosupport-brochure.PDF
Licence	Operační systém	Licence umožňující provoz virtuálního prostředí a min. 2 virtuálních serverů	Součástí dodávky serverů je i Windows Server 2022 v edici Standard umožňující provoz dvou virtuálních serverů stejné edice.	Součástí cenové nabídky

2.6 Požadavky na architekturu technického řešení

(1) **Architektura položek musí být navržena tak, aby vhodně využívala a doplňovala stávající systémy zadavatele veřejné zakázky.** Tento požadavek znamená, že nové řešení musí být kompatibilní s existujícími systémy zadavatele veřejné zakázky, přičemž musí efektivně integrovat a rozšiřovat jejich funkcionality bez nutnosti zásadních změn stávající infrastruktury.

2.7 Požadavky na kompatibilitu s ostatními systémy

(1) **Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí nabízené virtualizace P3 a musí být pro běh v tomto prostředí výrobcem podporovány.** To znamená, že jakýkoliv software dodávaný jako součást řešení musí být oficiálně podporován pro virtuální prostředí specifikované v P3. To zahrnuje ověření, že software bude bez problémů fungovat a bude plně kompatibilní s virtualizačními platformami, které jsou součástí P3.

2.8 Požadavky na typy klientů

(1) **Webová rozhraní nabízených systémů a zařízení musí být funkční v obvyklých internetových prohlížečích – min. MS Edge, Chrome, Safari v aktuálních verzích bez potřeby instalace speciálních doplňků či plug-in modulů.** Rozhraní musí být navržena tak, aby byla plně funkční v moderních webových prohlížečích bez potřeby instalace dodatečných komponentů. To zajišťuje širokou kompatibilitu a usnadňuje uživatelský přístup.

2.9 Požadavky na bezpečnost informací

(1) **Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na LDAP/Active Directory.** Nástroje musí umožňovat správu uživatelských účtů a poskytovat možnost integrace s existujícími autentizačními systémy, jako jsou LDAP nebo Active Directory, pro centralizovanou správu přístupu.

(2) **Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa).** Systémy musí podporovat víceúrovňový model oprávnění, který odděluje uživatelské role na úrovni pouze pro čtení a administrátorské úrovni s plným přístupem a schopností měnit konfigurace.

(3) **Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).** Zabezpečení komunikace mezi nástroji a zařízeními je klíčové. Všechny přenosy dat musí být šifrované pomocí bezpečných protokolů, aby se ochránily citlivé informace před neoprávněným přístupem.

3. Implementační služby

3.1. Obecné požadavky

(1) **Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Účastník je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci 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:**

(a) **Zajištění projektového vedení realizace předmětu plnění dle standardu Prince 2.**

Účastník musí zajistit projektové řízení v souladu se standardem Prince 2, který zahrnuje plánování, řízení a kontrolu projektu. To zahrnuje řízení časového plánu, rozpočtu, rizik a kvality.

(b) **Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.**

Dokumentace musí obsahovat všechny podklady potřebné k realizaci projektu, včetně předimplementační analýzy a detailního návrhu cílového stavu. Dokumentace musí vycházet z osvědčených praktik a doporučení výrobců technologií.

(c) **Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení.**

Účastník je povinen dodat a implementovat všechny prvky a technologie dle specifikace v prováděcí dokumentaci a technických parametrů.

(d) **Provedení školení.**

Školení musí být zajištěno pro relevantní osoby, aby byly schopné efektivně používat nové systémy a technologie.

(e) **Zajištění zkušebního provozu.**

Účastník musí provést zkušební provoz, aby se ověřila funkčnost a stabilita systému před jeho plným uvedením do provozu.

(f) **Provedení akceptačních testů.**

Akceptační testy musí být provedeny k ověření, že systém splňuje všechny požadavky a parametry specifikované v dokumentaci.

(g) **Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby, administrace systémů a činností pro spolehlivé zajištění provozu a obnovu systémů.**

Provozní dokumentace musí obsahovat podrobný popis toho, jak byl systém skutečně implementován a jaké činnosti jsou potřeba pro jeho údržbu a správu.

(h) **Předání do ostrého provozu.**

Po úspěšném dokončení všech předchozích kroků musí být systém předán do plného provozu, kde bude plně funkční a použitelný.

(2) **Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.**

Všechny náklady na implementační služby musí být zahrnuty v celkové ceně nabídky. Tyto náklady nelze uvádět samostatně.

(3) **Účastník je dále povinen zahrnout do nabídky i další související služby minimálně v dále uvedeném rozsahu. Pro každou uvedenou službu uvede účastník podrobný popis způsobu provedení služby při realizaci předmětu plnění zohledňující požadavky zadavatele na technické řešení.**

Účastník musí poskytnout detailní popis všech dalších souvisejících služeb, které jsou nezbytné pro úspěšnou realizaci projektu. Tento popis musí reflektovat technické požadavky zadavatele a zohledňovat všechny aspekty implementace.

P.1 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS MmM

Položka	Popis
a)	Analýza ICT prostředí se zaměřením na vyhledání a inventarizace privilegovaných účtů
b)	Upřesnění instalace, parametrizace, definování workflow, popis realizace integrace s navazujícími systémy
c)	Návrh DR v případě nedostupnosti řešení PIM/PAM
d)	Vybudování management (JUMP) serveru dle obecných best practices
e)	Implementace MS LAPS pro koncové stanice i servery
f)	Vybudování systému pro správu a řízení privilegovaných účtů
g)	Integrace s Active Directory (LDAP) a Email serverem Zadavatele
h)	Nastavení dvoufaktorové autentizace
i)	Integrace s operačními systémy serverů provozovaných Zadavatelem
j)	RDP protokol pro Windows platformu
k)	SSH protokol pro OS Linux/Unix platformu
l)	Vytvoření účtů pro kmenové zaměstnance Zadavatele a přiřazení oprávnění k příslušným serverům
m)	Vytvoření účtů pro externí pracovníky a přiřazení oprávnění k příslušným

	serverům
n)	Návrh a provedení akceptačních testů

P.2 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management, SIEM)

Položka	**Popis**
a)	Analýza a detailní identifikace zdrojů dat pro provozně bezpečnostní informace; návrh způsobu zpracování a proaktivních i reaktivních akcí
b)	Vybudování systému centrálního logování pro zaznamenávání činnosti systému, jeho uživatelů a administrátorů
c)	Napojení na nabízené SIEM řešení
d)	Návrh a provedení akceptačních testů, včetně testů archivace a obnovy logů a ověření detekce neoprávněných modifikací
e)	Předání technické dokumentace skutečného provedení
f)	Měsíční dohled, kontrola, vyhodnocení provozu SIEM v rozsahu 1 MD/měsíčně po dobu udržitelnosti projektu
g)	Zaškolení

P.3 - Nástroje pro zajišťování úrovně dostupnosti informací – HW pro zajištění provozu implementovaných řešení

Položka	**Popis**
h)	Analýza a detailní rozložení zdrojů dat pro jednotlivé provozované systémy
i)	Návrh zabezpečení infrastruktury, nezávislé na stávajících systémech (virtualizace, Active Directory apod.)
j)	Vybudování vysoce dostupného dvou nodového clusteru pro provoz nabízených systémů
k)	Implementace datového úložiště na dva nově dodané servery (hypervizory)
l)	Návrh a provedení akceptačních testů
m)	Předání technické dokumentace skutečného provedení
n)	Zaškolení

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

3.2. Požadavky na zpracování prováděcí dokumentace

(1) Účastník před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(2) Jako podklad pro zpracování prováděcí dokumentace provede účastník předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění účastníka, zejména pak s ohledem na účastníkem použité technické řešení, minimálně pro následující oblasti:

a. Analýza a vyhodnocení stávajícího stavu, identifikace slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy.
b. Způsob začlenění nabízených položek do prostředí zadavatele.
c. Síťová infrastruktura ve vztahu k plánovanému využití.

d. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
e. Analýza možností napojení zdrojových aplikačních systémů, resp. možností získávání jejich dat.
f. Integrace nabízených softwarových systémů.
g. Požadavky na rekonfiguraci stávajících systémů ve vztahu k plánovanému využití jejich dat.
h. Dopady implementace na dostupnost a funkčnost stávajících služeb.
i. Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
j. Integrace s virtualizační platformou ve vysoce dostupném režimu.
k. Požadované součinnosti Zadavatele.
l. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného účastníkem a musí obsahovat minimálně tyto části:

a. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému.
b. Nutné a doporučené optimalizační a konfigurační změny dodávaných systémů i všech navázaných systémů.
c. Způsob zajištění dodávek a služeb, včetně harmonogramu zajištění HW dodávek.
d. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem.
e. Detailní návrh a popis postupu implementace předmětu plnění.
f. Detailní popis zajištění bezpečnosti informací.
g. Detailní harmonogram projektu včetně uvedení kritických milníků.
h. Vazby na stávající systémy a jejich konfigurace.
i. Návrh akceptačních kritérií a akceptačních testů.
j. Detailní popis navrhovaných školení.
k. Komunikační schéma.
l. Obsah a rozsah provozní dokumentace.

(4) Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání dodavatelem připomínkována objednatelem a připomínky budou ze strany dodavatele vypořádány v co nejkratší době s nástupem vypořádání do 2 pracovních dní (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na dodavateli jejich řádné zpracování.
(5) Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem.
(6) Na základě provedené implementace bude prováděcí dokumentace aktualizována na skutečně provedenou včetně detailní konfigurace, a to jak funkční, tak provedené nastavení včetně podložení provedenými analytickými podklady a dokumenty. Aktualizovaná prováděcí dokumentace bude součástí dokumentace předávané v rámci předávacího protokolu.

3.3. Harmonogram realizace

(1) Účastník 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.

(2) Zadavatel vyžaduje navržení následujícího harmonogramu plnění – kde účastník uvede maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo, čísla značí počet kalendářních dnů. Celková aktivita projektu musí být v souladu s podmínkami Výzva č. 41 - Kybernetická bezpečnost – pro obce z Národního plánu obnovy a nesmí je překročit, musí být dokončena v dostatečném předstihu, a to do 34 týdnů od nabytí účinnosti smluvního vztahu.

Poř. č.	**Aktivita projektu**	**Nejpozdější termín pro dokončení aktivity**
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+90
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+110
E1.4	Dodávky a implementace	D+170
E1.5	Školení uživatelů a administrátorů	D+190
E1.6	Zkušební provoz	D+200
E1.7	Akceptační testy	D+220

(3) Maximální lhůtu trvání nesmí účastník při tvorbě detailního harmonogramu prodloužit.

(4) Účastník uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.

(5) Účastník uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

3.4. Požadavky na školení

(1) Účastník 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.

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

a. Školení administrátorů – minimální rozsah školení je 16 hodin na každou položku (P). Předpokládá se účast maximálně 5 osob, školení bude probíhat v sídle Zadavatele. Zadavatel může změnit místo školení dle potřeby.

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

(4) Formát školení musí být 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.

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

(1) Účastník navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny položky (P) vždy zahrnovat minimálně:

a. Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.
b. Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
c. Prokázání aktivace softwaru i hardwaru aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
d. Prokázání registrace/aktivace podpory hardware a software výrobce, pokud je podpora součástí dodávky a její aktivace je potřebná.
e. Pro každou položku (P) navrhne účastník vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a stabilita dodaného řešení.
f. Výkonové testy prokazující shodu s požadovanými výkonnostními parametry a dále výrobcem deklarovanými či s ohledem na technologii objektivně očekávatelnými parametry, např. výkon u datových úložišť (IOPS, přenosová rychlost, latence).

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

(3) Účastník zajistí pro každou položku (P) zkušební (testovací) provoz v délce minimálně 14 dnů, včetně technické podpory minimálně 1 specialisty na dodané řešení, s dojezdem maximálně 1 hodiny od nahlášení požadavku v pracovní den v době od 8:00 do 17:00.

3.6. Požadavky na dokumentaci

(1) Účastník zpracuje provozní dokumentaci, která detailně popisuje konfiguraci zhotoveného díla a jeho vazby na stávající systémy. Dokumentace bude zahrnovat podrobnosti o architektuře, použitých technologiích a specifických nastaveních, která byla použita během implementace. Dále bude obsahovat popis všech integrací s existujícími systémy a procesy, včetně schémat a diagramů, které usnadní porozumění a údržbu. V rámci provozní dokumentace bude rovněž zahrnuta část zaměřená na disaster recovery (obnova po havárii). Tato část bude obsahovat:

a. Plán obnovení po havárii: Detailní kroky pro obnovu funkcionality zhotoveného díla v případě výpadku nebo havárie. Plán bude zahrnovat

scénáře různých typů havárií, jako jsou výpadky hardwaru, selhání softwaru, nebo kybernetické útoky.

b. Zálohovací strategie: Informace o pravidelných zálohách dat a konfigurací, včetně popisu metod a frekvence zálohování. Dokumentace bude specifikovat umístění záloh (lokální, vzdálené, cloudové) a postupy pro jejich obnovení.
c. Obnova systémů: Krok za krokem postup pro obnovu jednotlivých komponentů systému včetně nezbytných kroků k zajištění integrity a dostupnosti dat po havárii.
d. Testování a údržba plánu: Plán pravidelných testů obnovy, které ověří účinnost a aktuálnost disaster recovery plánu. Budou zahrnuty instrukce pro údržbu a aktualizaci plánu v případě změn v systému nebo jeho komponentách.
e. Kontakty a eskalační postupy: Seznam klíčových kontaktů pro technickou podporu a eskalační postupy v případě vážných incidentů, které nelze vyřešit standardními postupy.

Tato část dokumentace zajistí, že všechny zúčastněné strany budou mít jasné pokyny a postupy pro minimalizaci dopadů případných problémů a pro rychlé obnovení normálního provozu systému.

(2) Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizována podle skutečného stavu.
(3) Součástí provozní dokumentace bude popis úkonů doporučené údržby, specifikace intervalů jejího provádění a další dokumentace v rozsahu stanoveném v prováděcí dokumentaci.
(4) Dokumentace bude dodána v elektronické podobě, která umožňuje její zobrazení a čtení prostřednictvím běžných nástrojů, jako je kancelářský balík nebo ve formátu PDF.

4 Technická podpora a služby

(1) Měsíční dostupnost (SLA): 98,00 %. V případě nedodržení měsíční dostupnosti (SLA) dojde ke snížení měsíční ceny technické podpory podle níže uvedené tabulky a vzorce:

Měsíční dostupnost (SLA)	**Sleva z měsíční ceny technické podpory**
97,99 % - 97,00 %	10 %
96,99 % - 95,00 %	15 %
Méně než 95,00 %	30 %

$$Dostupnost\ (\%) = \left(1 - \frac{celkový\ čas\ výpadků\ (minuty)}{\text{celkový čas meření (minuty)}}\right) x100$$

(2) Online Helpdesk pro řešení provozních problémů a ohlášených incidentů, který je součástí technické podpory.

(3) Technická podpora musí být poskytována výhradně v českém jazyce.

(4) Proaktivní údržba, aktualizace a optimalizace systémů je součástí technické podpory.

(5) Vzdálený přístup dodavatele do prostředí objednavatele prostřednictvím VPN připojení.

(6) Telefonická asistence dodavatele v rozsahu 16 hodin měsíčně je součástí technické podpory. Nevyčerpané hodiny budou převáděny do následujícího měsíce, přičemž převedené hodiny vyprší na konci kalendářního roku.

(7) Doby plnění podle níže uvedené tabulky se sankcemi (smluvními pokutami) za jejich nedodržení.[2]

Druhy požadavků	**Zpětná reakce (potvrzení obdržení požadavku)**	**Zahájení zásahu**	**Další specifikace**	**Vyřešení**
Závada	Do 2 hodin od nahlášení nebo zjištění závady	Do 2 hodin od nahlášení nebo zjištění závady	Do 10 hodin od nahlášení nebo zjištění závady, nebude-li dohodnuto jinak	Do 30 hodin od nahlášení nebo zjištění závady, pokud není dohodnuto jinak. Sankce: 100 Kč za každou hodinu prodlení.
Servisní požadavek	Do 2 hodin od nahlášení požadavku	Do 2 hodin od nahlášení požadavku	Do 10 hodin od nahlášení požadavku	Do 50 pracovních hodin od nahlášení požadavku, pokud není dohodnuto jinak. Sankce: 100 Kč za každou hodinu prodlení.
Změnový požadavek	Do 8 hodin od nahlášení požadavku	N/A	Do 10 pracovních dnů od nahlášení požadavku, předložit návrh řešení, pokud není dohodnuto jinak.	Dle dohody. Sankce: 1000 Kč za každý den prodlení.
Požadavek na konzultační služby	Do 8 hodin od nahlášení požadavku	N/A	Do 15 pracovních dnů od nahlášení požadavku, poskytnout	Dle dohody. Sankce: 1000 Kč za každý den prodlení.

[2] Doby plnění se počítají pouze v pracovní době systému (pracovní hodiny) od 8:00 do 17:00. Pro účely sankcí se délka prodlení počítá také pouze v pracovní době.

			konzultaci, pokud není dohodnuto jinak.	

- Pokud bude rozsah závady takový, že nebude možné provést nápravu obvyklými prostředky, musí dodavatel do 24 hodin od nahlášení závady navrhnout náhradní řešení, jehož realizaci objednatel bezodkladně zváží s ohledem na možné poškození jeho zájmů.
- Zajištění záručního servisu technologií nebo předmětu plnění je součástí technické podpory.
- Cena technické podpory zahrnuje pravidelné profylaxe prostředí a to minimálně jednou ročně.
- Cena technické podpory zahrnuje bezodkladné aktualizace prostředí v případě zjištění bezpečnostní hrozby, která může ohrozit informační systém objednatele (všechny komponenty, které využívá aplikační prostředí, a nejsou součástí operačního systému, který si sám aktualizuje zadavatel VZ). Bude klasifikováno podle SLA jako závada.
- Určení druhu požadavku náleží objednateli.
- Servisní požadavky budou plněny přednostně v pracovní době (pracovní dny od 8:00 do 17:00), v takovém případě je cena za jejich plnění součástí ceny technické podpory.

Cena technické podpory zahrnuje všechny náklady na poskytování technické podpory, včetně nákladů spojených s technickou podporou a garancí nástupu servisního technika (zahájení zásahu).