Příloha č. 1: Nabídka dodavatele

	Cena za jednotku/ Kč	Počet ks	jednotka	Cena celkem bez DPH	Cena s DPH
Log management- Licence: TeskaLabs LogMan.io Municipality edition	718 028,-	1	sw	718 028,-	868 813,88
Log management- Maintenance TeskLabs Logman.io Municipality edition - roční podpora	145 600,-	5	sw	728 000,-	880 880,-
Log management- hw	200 000,-	2	hw	400 000,-	484 000,-
Konfigurační a implementační práce	16 000,-	12	MD	192 000,-	232 320,-
Školení	15 000,-	2	MD	30 000,-	36 300,-
Rozšířená podpora- 100hod v období 60měsíců	80 000,-	1		80 000,-	96 800,-
Cena celkem (Kč)				**2 148 028,-**	**2 599 113,88**

Příloha č. 2: Technická specifikace pro část pro část B Log management

TECHNICKÁ SPECIFIKACE – část B Log management (centralizované logování)
Zajištění kybernetické bezpečnosti na MěÚ Vyškov

1. Úvod

Tato část řeší dodání nástroje pro centralizovaný sběr, správu a vyhodnocování logovacích záznamů z infrastrukturních prvků Městského úřadu Vyškov. Požadované řešení musí podporovat korelaci událostí, pokročilou vizualizaci, detekci anomálií a generování reportů. Důraz je kladen na kompatibilitu se standardními logovacími protokoly (Syslog, SNMP, WEC/WEF apod.) a na soulad s legislativou (např. NIS2, zákon č. 181/2014 Sb.).

Uchazeč dodá kompletní řešení včetně veškerých licencí a podpory na dobu 5 let. Řešení bude provozováno samostatně, bez zatěžování existující infrastruktury zadavatele, a musí zajistit vysokou dostupnost. Všechny požadované funkcionality musí být dostupné v okamžiku podání nabídky a doloženy formou kompletní technické specifikace.

2. Technická specifikace

2.1 Vymezení

Tato část veřejné zakázky definuje technické, provozní a kvalitativní požadavky na poptávané řešení, které tvoří součást projektu modernizace a posílení kybernetické bezpečnosti Městského úřadu Vyškov. Uchazeč je povinen předložit nabídku, která bude funkčně a parametricky odpovídat této specifikaci a současně naplní veškeré cíle stanovené zadavatelem pro danou oblast.

Předmětem plnění je dodávka kompletního řešení zahrnujícího nejen vlastní produkt, ale i všechny nutné komponenty, licence, služby, dokumentaci, implementaci a školení uživatelů, a to v rozsahu nezbytném pro jeho plnohodnotné a bezpečné zprovoznění. Všechna nabízená řešení musí být nová, určená pro trh EU, s plnou podporou a zárukou výrobce, bez využití tzv. druhotných licencí.

Uchazeč zahrne do své nabídky veškeré náklady na dodávku, instalaci, zprovoznění a následnou podporu. Pokud technická specifikace obsahuje tabulky určené pro doplnění, je uchazeč povinen je řádně vyplnit. Nesplnění uvedených podmínek může být důvodem pro vyloučení nabídky. Zadavatel si vyhrazuje právo prověřit původ výrobků při jejich předání, včetně kontroly sériových čísel a potvrzení formou akceptačního protokolu.

2.2 Specifikace

Specifikace je popsána v Příloze č. 4 Smlouvy o dílo a smlouvy o poskytování servisní podpory, jako její nedílná součást.

2.3 Všeobecná pravidla

Zadavatel požaduje dodávku dále uvedeného zboží, a to jako zboží nové, nikoliv demo, repasované nebo jakkoliv již dříve použité. Zadavatel níže specifikované zboží požaduje v uvedených počtech kusů.

Zboží musí splňovat veškeré technické požadavky stanovené pro jeho uvedení na trh a do provozu dle právních předpisů, zejména zákona č. 22/1997 Sb., o technických požadavcích na výrobky ve znění pozdějších předpisů.

Pokud je v technické specifikaci níže užit pojem „možnost", rozumí se tím vlastnost, funkce či schopnost zboží, nikoliv pouze jeho připravenost k využití této možnosti (tzn. že zadavatel požaduje, aby mohl tyto „možnosti" využívat bez dalších finančních investic do různých rozšíření, upgradů apod., nejsou-li tyto výslovně zmíněny).

Zadavatel vyžaduje, aby nabízená zařízení splňovala následující požadavky:

- Veškeré dodávané HW a SW produkty byly získány legálně a umožňují využití těchto zařízení zadavatelem jako koncovým zákazníkem v souladu s distribučními a licenčními podmínkami výrobce zařízení;
- Po dodání HW a SW produktů zadavateli jako koncovému zákazníkovi nesmí být zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje, což musí zahrnovat i nárok zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání smlouvy;
- V databázi výrobce musí být zadavatel veden jako koncový uživatel zboží a licencí/subskripcí/operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh – certifikace CE;

2.4 Ostatní požadavky

Dodavatel zajistí kompletní integraci systému s minimálně těmito prvky: servery, koncové stanice, Active Directory, firewall, NAS úložiště, síťové prvky.

Součástí bude dodání HW prostředí nebo specifikace virtuální appliance s odpovídajícím výkonem (provoz mimo stávající servery zadavatele).

Řešení bude zahrnovat detailní technickou dokumentaci v českém jazyce a proškolení správce systému (min. 4 hodiny).

Dodavatel zajistí import historických logů a základní přizpůsobení dashboardu podle potřeb zadavatele.

Požaduje se možnost napojení na nadřazený SIEM nebo export do externího úložiště.

4. Implementační služby

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

Zajištění projektového vedení realizace předmětu plnění.

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

Provedení školení,

Zajištění zkušebního provozu,

Provedení akceptačních testů,

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

Předání do ostrého provozu,

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

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

4.1 Harmonogram realizace

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

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

HARMONOGRAM

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

jednotka = 1 den

Dodavatel může dle svého uvážení výše uvedené maximální lhůty zkrátit

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

4.2 Požadavky na školení

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

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

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

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

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

4.3 Požadavky na provedení akceptačních testů

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

Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

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

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

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

Dodavatel zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 14 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h. Dojezd do 2 hodin od nahlášení požadavku (v rámci pracovní doby) je zásadní pro udržení provozu kritických informačních systémů v potřebném rozsahu při plnění zákonných povinností zadavatele. V případě předávání díla po částech je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

4.4 Požadavky na dokumentaci

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

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

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

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

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

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

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

5. Požadavky na záruky a MAINTENANCE

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně 36 měsíců od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Dodavatel ve své nabídce uvede ceny záruky takto:

Standardní záruka a standardní podpora běžně poskytovaná výrobcem infrastrukturní technologie na území České republiky = 3ROKY bude součástí pořizovací ceny zařízení.

Cenu záruk pro 5 let projektu a nadstandardních podpor (včetně aktualizací software/firmware apod.) požadovaných Zadavatelem (tj. rozdíl mezi Standardními zárukami 3ROKY a podporami a požadavky Zadavatele) dodavatel uvede v položce "Nadstandardní záruky a podpory výrobců"

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

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

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

- Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
- Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
- Perfekcionistická údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.
- Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

6. Požadavky na podporu provozu

6.1 Obecná pravidla provozu

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

Provozní doba helpdeskového systému pro zadávaní požadavků musí být 24x7.

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

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

6.2 Požadavky na podporu provozu

Rozsah základní servisní podpory (ZSP):

Provádění aktualizací firmware a software dodaných produktů (nezahrnuje upgrade na nové hlavní verze software) v rozsahu 2 hod měsíčně. Četnost aktualizací řídí Dodavatel s ohledem na zajištění spolehlivého provozu systémů a jejich bezpečnost a kritičnost aktualizací.

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

Rozsah rozšířené servisní podpory (RSP):

Řešení Incidentů – pokud se během řešení Incidentu ukáže, že se jedná o vadu, která spadá pod záruku systému, nebude se čas potřebný pro řešení incidentu Zadavateli účtovat.

Řešení Incidentů může být zahájeno na základně požadavku Zadavatele, na základě Zadavatelem schváleného požadavku třetí strany nebo na základě schváleného podnětu dodavatele.

Odborná podpora – vzdálené konzultace pro podporované služby/produkty

Pro případ, že bude zadavatel požadovat služby rozšířené servisní podpory podle odst. (2), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci

ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené servisní podpory pro účely přípravy nabídky je 100 hodin / 60 měsíců.

6.3 Požadavky na podporu provozu

Servisní podpora je poskytována zejména následujícím způsobem:

Prostřednictvím pracovníka dodavatele Vzdálenou správou

Prostřednictvím pracovníka dodavatele přímo na pracovišti Zadavatele

Prostřednictvím pracovníka dodavatele formou vzdálené konzultace

Dodavatel provede záznam o provedení servisní podpory, v záznamu uvede relevantní informace včetně doby poskytování servisní podpory a záznam zašle elektronicky zadavateli. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

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

- zajistit a udržovat podmínky pro Vzdálený přístup dodavatele,

- zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,

- zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku dodavatele veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,

- umožnit dodavateli v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,

- zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné (na výzvu takovou potřebnost písemně odůvodní).

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

Zadavatel je dále v rámci součinnosti povinen

elektronicky potvrdit dodavateli provedení služby,

zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,

poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí (pokud tyto nepochází od dodavatele).

6.4 Postup při řešení incidentů

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

Incident:

Kritický: Incident, při kterém dojde k selhání funkcionalit systému LOGmanager, jež znemožní detekci nebo řádné ohlášení bezpečnostního rizika v rámci stanoveného časového rámce dle SLA. Takové selhání může vést ke ztrátě, neoprávněnému přístupu, úniku nebo narušení integrity citlivých dat, a má přímý dopad na plnění smluvních povinností v oblasti informační bezpečnosti.

Nekritický: Událost, při níž dojde k drobnému technickému nebo provoznímu nedostatku v systému LOGmanager (např. opožděné doručení méně důležitého logu, dočasná nedostupnost neklíčové komponenty), která však nemá přímý dopad na bezpečnost, dostupnost nebo integritu zpracovávaných dat a neohrožuje plnění smluvních povinností.

Součástí nahlášení požadavku Zadavatelem musí být:

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

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

Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 2 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 8:00 a 17:00 v pracovní dny.

Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.

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

Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

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

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši

náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

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

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

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

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

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

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

6.5 Záruky na servisní služby

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

Příloha č. 3 Cena

1. **Cena – Log management**

1.1. Cena plnění (dílo a služby servisní podpory) je stanovena následovně:

Popis	Počet	Ceny v Kč bez DPH za počet				Celková cena v Kč s DPH
		HW	SW (Licence)	Podpora + maintenance celkem 60 měsíců (5 let)	Celková cena	
Zboží						
Log management - nástroj	1	400.000,-Kč	718.028,-Kč	728.000,-Kč	1.846.028,- Kč	2.233.693,88Kč
Montáž a konfigurace	1				192.000,-Kč	232.320,- Kč
Dokumentace					0,-Kč	0,-Kč
Školení	1				30.000,- Kč	36.300,- Kč
Služby rozšířené servisní podpory	100 hodin za 60 měsíců				80.000,- Kč	96.800,- Kč

Celková cena v Kč bez DPH	2.148.028,- Kč
Celková cena v Kč s DPH	2.599.113,88 Kč

Příloha č. 4: Technické požadavky na plnění

Příloha č. 3B: Technické požadavky na plnění (část B Log management)

LOG management

2 KS

Parametr	Požadované funkcionality/vlastnosti	Splněno ANO / NE	Popis splnění požadavku
	Výrobce a model		**TeskaLabs LTD, odštěpný závod, LogMan.io municipality edition**
Obecné požadavky			
ZÁKLADNÍ TECHNICKÉ POŽADAVKY	Řešení je postaveno na architektuře vysoké dostupnosti (HA cluster) s podporou active-active provozu a bez single point of failure.	ANO	Řešení je navrženo jako HA cluster v režimu active-active, bez single point of failure. Ingest, zpracování, indexace, analytika i úložiště běží redundantně; výpadek uzlu nemá vliv na příjem ani dostupnost dat.
	Nasazení je on-premise, podporované jako virtuální appliance pro platformy VMware, Microsoft Hyper-V a KVM, případně jako HW appliance.	ANO	Nasazení je on-premise. Dodáváme jako virtuální appliance pro VMware, Microsoft Hyper-V a KVM, případně jako předinstalovanou HW appliance dle kapacitních požadavků.
	Řešení je odolné vůči výpadku datového centra a umožňuje provoz na více lokalitách.	ANO	Řešení podporuje provoz na více lokalitách a je odolné vůči výpadku datového centra. Geo-distribuce uzlů zajistí zachování příjmu a provozu i při ztrátě celé jedné lokality.
	Logy jsou přesměrovány na virtuální IP, která zajišťuje přepojení bez zásahu administrátora.	ANO	Logy jsou směrovány na virtuální IP adresu clusteru. VIP se při failoveru automaticky přesouvá mezi uzly; přepnutí nevyžaduje zásah administrátora ani změny na zdrojích.
	Archivační úložiště má kapacitu minimálně 2× 100 TB, oddělené pro systémová a logová data.	ANO	Archivační vrstva je oddělena pro systémová a logová data, s kapacitou minimálně 2× 100 TB. Podporujeme lokální pole, NAS/SAN i škálování kapacity přidáním shelfů.
	Minimální limit pro příjem logů je 5 GB denně, s možností licenčního navýšení této kapacity.	ANO	Minimální garantovaný příjem je 5 GB/den a lze jej licenčně navyšovat. Při překročení objemu nedochází ke ztrátě dat: systém příjem neomezuje a administrátora upozorní.
	Řešení podporuje min. 4× vNIC pro síťovou separaci (např. management, ingest, archivace, monitoring).	ANO	Každá instance podporuje minimálně 4× vNIC pro síťovou separaci (management, ingest, archivace, monitoring). Rozhraní lze mapovat do samostatných VLAN a řídit QoS.
	Umožňuje provozovat systém také jako úložiště logů bez další analýzy z vybraných zdrojů.	ANO	Systém lze provozovat jako čisté úložiště logů bez analýzy pro vybrané zdroje. Data jsou přijata, chráněna a archivována s možností pozdějšího dohrání do analytické vrstvy.
	Sběr logů je distribuovaný, s podporou Syslog, SNMPv2/v3, REST API, WEC/WEF, JSON, Windows EventLog, bez nutnosti agentů.	ANO	Sběr logů je distribuovaný a bezagentní: Syslog (RFC 3164/5424/3195/6587), SNMPv2/v3, REST API, WEC/WEF, Windows EventLog, JSON a další běžné formáty. Kolektory mají perzistentní buffer pro dočasnou ztrátu konektivity.
	Přenos logů je šifrován pomocí Mutual TLS, integrita logů je ověřována digitálním podpisem.	ANO	Přenos logů je šifrován pomocí Mutual TLS s obousměrným ověřením. Integrita je ověřována digitálním podpisem a každá událost má jednoznačný identifikátor.
	Multi-tenancy režim, oddělené datové prostory a granulární RBAC oprávnění.	ANO	Systém podporuje multi-tenancy s fyzickým i logickým oddělením datových prostorů. Přístupy jsou řízeny granulárním RBAC na úrovni tenantů, zdrojů, typů dat i funkcí.
	Mikroservisová architektura, podpora rolling upgrade bez výpadku, správa konfigurace s možností verzování (např. Git).	ANO	Mikroservisová architektura umožňuje rolling upgrade bez výpadku služeb. Konfigurace je verzována (např. Git), s možností auditního náhledu a rychlého rollbacku.
	Výkon: min. 2 000 EPS v běžném režimu, až 8 000 EPS ve špičce po dobu 60 minut, bez ztráty dat.	ANO	Výkon: min. 2 000 EPS v běžném provozu na navržené konfiguraci; až 8 000 EPS ve špičce po dobu 60 minut bez ztráty dat díky škálování ingestu a perzistentním frontám.
	Uchovávání logů: 6 měsíců online, 18 měsíců archiv s možností exportu na NAS/SAN, pásky, nebo do cloudových úložišť (Azure, AWS).	ANO	Uchovávání: 6 měsíců online pro okamžité vyhledávání, 18 měsíců v archivu. Export archivu na NAS/SAN, pásky a do cloudových úložišť Azure a AWS je podporován.
	Retenční politika podle typu logu, úrovně důvěryhodnosti nebo klasifikace.	ANO	Retenční politika je definovatelná podle typu logu, úrovně důvěryhodnosti i klasifikace. Pro každou skupinu lze nastavit vlastní zásady hot/archiv a přesuny mezi úložišti.
	Logy zůstávají dostupné i při výpadku samotného systému logování.	ANO	Logy zůstávají dostupné i při výpadku části systému logování. Kolektory uchovají data v perzistentním bufferu a úložiště je replikované; po obnově dojde k automatickému doposlání.
	Fulltextové vyhledávání, korelace událostí, kategorizace, zobrazení RAW logů a vizualizace dat.	ANO	Vyhledávání je fulltextové nad všemi poli, systém podporuje korelace, kategorizace a zobrazení RAW zprávy paralelně se strukturovanou podobou. Data jsou vizualizována v dashboardech a grafech.
	Možnost reálného času zobrazení aktuálních logů z jednotlivých NGFW zařízení a zpětné analýzy provozu minimálně 7 dní.	ANO	Konzole zobrazuje logy z NGFW v reálném čase (live tail) a umožňuje zpětnou analýzu minimálně 7 dní v hot úložišti bez reimportu. Filtry a drill-down jsou dostupné okamžitě.
	Detekce hrozeb pomocí pravidel (včetně podpory Sigma rules) a analýzy anomálií pomocí strojového učení z historických dat.	ANO	Detekce hrozeb pomocí pravidel a podpory Sigma rules, doplněná o analýzu anomálií strojovým učením nad historickými daty. Podporujeme korelace v časových oknech i TI seznamy.
	Možnost automatizovaných reakcí na zjištěné hrozby přímo z grafického rozhraní, včetně napojení na NGFW.	ANO	Automatizované reakce lze spustit přímo z GUI a navázat na NGFW. Integrace probíhá přes REST API nebo nativní konektory (např. blokace IP, úprava politik, aktualizace seznamů).
	Generování komplexních reportů (např. Top X zařízení, přenos, hrozby), reporty na základě dotazů do databáze.	ANO	Systém generuje komplexní reporty včetně Top X zařízení/přenosů/hrozeb a reportů z uživatelských dotazů. Reporty lze skládat z tabulek, grafů a uložených pohledů.
	Formáty reportů: HTML, CSV, XML, PDF. Možnost automatického plánování a zasílání.	ANO	Formáty reportů: HTML, CSV, XML, PDF. Podporujeme plánování, periodické spouštění a distribuci na e-mail či síťové úložiště.
	Možnost brandování reportů (loga, hlavičky, patičky).	ANO	Reporty lze brandovat (loga, hlavičky, patičky) na úrovni tenantu i celého systému.
	Uživatelské rozhraní s možností světlého/tmavého režimu, samostatná sekce pro zobrazení zjištěných hrozeb.	ANO	Uživatelské rozhraní podporuje světlý/tmavý režim a obsahuje samostatnou sekci pro zjištěné hrozby s filtrováním, drill-downem a napojením na alert management.
	Soulad s požadavky NIS2, zákonem č. 181/2014 Sb., vyhláškou č. 82/2018 Sb. a doporučeními NÚKIB, včetně oblasti kryptografie.	ANO	Řešení je navrženo s důrazem na soulad s veškerými relevantními legislativními, regulatorními a metodickými požadavky, které jsou aktuální v České republice i na úrovni Evropské unie. Zvláštní důraz je kladen na požadavky vyplývající z evropské směrnice NIS2, zákona č. 181/2014 Sb., o kybernetické bezpečnosti, jeho prováděcí vyhlášky č. 82/2018 Sb., a doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), zejména v oblasti kryptografických prostředků.
POŽADAVKY NA MANAGEMENT	Centrální správa přes grafické rozhraní i CLI rozhraní.	ANO	Centrální správa je dostupná přes webové GUI i CLI. Všechny změny jsou auditované, rozhraní je zabezpečeno a víceuživatelské.

	Přístup přes REST API, včetně možnosti integrace s externími systémy.	ANO	Přístup je možný přes REST API pro integrace s externími systémy (ITSM, SOAR, monitorovací nástroje). API je autentizované, šifrované a dokumentované.
	Samostatná sekce v grafickém rozhraní pro zobrazení zjištěných hrozeb	ANO	Samostatná sekce hrozeb v GUI zobrazuje detekce, stav, trend a časovou osu, včetně souvisejících událostí a možností eskalace.
	Možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a NGFW zařízením	ANO	Komunikaci mezi analytickým řešením a NGFW šifrujeme (HTTPS/TLS, Mutual TLS) a autentizujeme certifikáty. Podporujeme bezpečné konektory výrobců NGFW.
POŽADAVKY NA PODPORU VÝROBCE	Podpora výrobce v režimu 24×7 na systém i konfiguraci je součástí nabídky.	ANO	Podpora výrobce v režimu 24×7 na systém i konfiguraci je součástí nabídky.
ZÁRUKA	Záruka na dodané řešení minimálně 36 měsíců, zahrnující technickou podporu, aktualizace a servisní zásah v případě poruchy.	ANO	Záruka na dodané řešení je minimálně 36 měsíců, zahrnující technickou podporu, aktualizace a servisní zásah v případě poruchy.
Produktové číslo	Part number SW - TL-LMIO-MUNED-LIC-2508 Part number HW TL-LMIO-HWU20-2508		
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://docs.teskalabs.com/logman.io/cs/		

tato pole musí být vyplněna dodavatelem

[redacted]