Specifikace plnění

Předmětem Veřejné zakázky je rozšíření komplexního managementu pro sběr a analýzu logů do technologických sítí Zadavatele.

Nabízené řešení musí být plně kompatibilní a integrovatelné se stávajícím systémem komplexního managementu pro sběr a analýzu logů provozovaném na platformě Logmanager od výrobce Logmanager a.s., dříve LOGmanager od výrobce Sirwisa a.s.

Obecné požadavky na celé řešení	**Nabízené řešení splňuje ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Zadavatel si v případě nejasnosti technických parametrů vyhrazuje právo otestovat jakýkoliv z požadavků v rámci PoC testu, který bude proveden před uzavřením kupní smlouvy na náklady Uchazeče, a to v rozsahu nezbytně nutném	ANO	V případě že vznikne požadavek zadavatele (či jeho hodnotící komise) v průběhu posuzování a hodnocení nabídek, je účastník připraven na výzvu zajistit příslušné komponenty pro řádné otestování v rámci PoC. Nicméně se domníváme, s ohledem na fakt, že nabízené produkty výrobce Logmanager, které jsou s prostředí zadavatele již nasazeny, že řešení je již otestováno dokonce v produkčním prostředí ŘSD.
Na každou část řešení musí být poskytnuta podpora výrobce jak na software, tak hardware, všechny licence a související po dobu 5 let od předání. Výměna vadného hardware musí být v režimu 8x5 NBD. Při nedodržení parametru výměny vadného hardware ŘSD náleží sankce 1 ‰ z ceny zařízení za každý započatý den zpoždění	ANO	Nabízené řešení je kryto rozšířenou zárukou / podporou výrobce na období 5 let. Centrální část pro log management (Logmanager XL) ... Logmanager-XL SW renewal Log forwardery do vzdálených lokalit (Logmanager HF) ... Logmanager-HF SW renewal
Veškeré komponenty celého řešení musí být nezávislé na virtualizačním prostředí zadavatele. Musí tak být dodány jako HW appliance	ANO	Ve všech případech se jedná o hardwarové appliance
U každé požadované funkcionality musí být uveden odkaz do veřejně dostupné dokumentace, případně do dokumentace vytvořené dodavatelem, kde je jasně popsán způsob plnění daného parametru. Tyto informace budou využity zadavatelem ke kontrole plnění tohoto parametru	ANO	Dokumentace výrobce je dostupná na webových stránkách výrobce https://logmanager.com/cs/zdroje/ Pracovníci zadavatele do ní mají již dnes přístup, jelikož nabízená technologie je již v prostředí sítě zadavatele nasazena a provozována.

Technické požadavky na Centrální část řešení pro log management	**Nabízené řešení splňuje ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Výrobce a model nabízeného produktu:		Logmanager
P/N a další specifikace nabízeného produktu:		LOGM-XL-200-4H ... Logmanager-XL doplněno o: LOGM-QUAD-SFP+- 4 portová SFP+ karta pro Logmanager XL + 4 ks optických transceiverů SR
Typ - HW Appliance do Racku včetně systému pro servisní manipulaci (výsuvné řešení)	ANO	Logmanager-XL je řešení založené na HW appliance, která je technicky založena na HW serveru o velikosti 2U se dvěma nezávislými napájecími zdroji. Řešení je vybaveno výsuvnými ližinami pro servisní manipulaci s HW appliancí.
Systém podporuje redundantní napájení - dva nezávislé zdroje, včetně napájecích kabelů	ANO	2x hot-swap napájecí zdroj včetně napájecích kabelů
Připojení do LAN - Redundantní, pomocí agregace min. 2 fyzických portů SFP+ pro sběr logů. Dedikovaný port pro správu HW RJ45	ANO	LOGM-QUAD-SFP+- datová komunikace je zajištěna
Optické členy SFP+ 10GBase-SR jako součást dodávky, metalický kabel RJ45 min. CAT6 délky 5m jako součást dodávky	ANO	LOGM-QUAD-SFP+-New - součástí karty jsou požadované SR transceivery Metalický kabel pro připojení managementu je rovněž součástí nabízeného řešení
Systém umožňuje vzdálenou správu HW včetně potřebné licence (obdoba HP iLO, DELL iDRAC, ...)	ANO	Management serveru je zahrnut v nabídce
Centrální část řešení musí umožňovat fungování v režimu vysoké dostupnosti (HA) při použití dvou a více prvků centrální části při zachování požadavků na výkon	**ANO**	**HA cluster se sestavuje ze dvou shodných appliancí (cluster lze rozšiřovat až do počtu čtyř nódů) - řešení umožňuje vytvoření clusterů až do 4 jednotek, které podporují více než 10 000 EPS. Kapacita databáze clusteru se rovná součtu kapacit všech jednotek clusteru děleno dvěma.**
Celkový počet zalicencovaných zařízení pro sběr logů - min. 50 000 zařízení	ANO	Více jak 50.000
Počet logů za vteřinu trvale - min. 10 000 logů za vteřinu	ANO	Více jak 10.000 EPS - Maximální udržitelný výkon měřený v událostech za sekundu (EPS) pro jednotku Logmanageru (Max Constant EPS). Směs surových logů s průměrnou velikostí 700 bajtů, testováno s plným parsováním.
Počet logů za vteřinu ve špičce (po dobu min. 5 minut) - min. 20 000 logů za vteřinu	ANO	Více jak 200.000 EPS - Peak EPS se rovná dvojnásobku Max Constant EPS po dobu 10 minut.
Celkový objem uložených logů - min. 200TB	ANO	200 TB - model LOGM-XL-200-4H je vybaven příslušným úložištěm
Období, po které budou uchovávány logy - min. 18 měsíců nebo do naplnění kapacity	ANO	Řešení zahrnuje neomezený počet agentů, zdrojů a systémových uživatelů - limit na dobu uchovávání logů je pak dán pouze kapacitou diskového systému úložiště.
Redundance pro výpadek minimálně dvou fyzických disků, bez dopadu na kapacitu a výkon řešení	ANO	Diskové úložiště je chráněno proti výpadku až 2 disků s využitím RAID 6
Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO	Jedná se o standardní součást nabízeného řešení

Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci software minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO	Jedná se o standardní součást nabízeného řešení v návaznosti na předplacenou 5-letou podporu výrobce
Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware, minimálně ze zařízení v Příloze Zdroje logů (list Zdroje logů)	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení Dokumentace výrobce je dostupná na webových stránkách výrobce
Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL, a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém provádí konsolidaci logů na interním storage logovacího systému.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém provádí automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém podporuje nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
V případě krátkodobého (do 5 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 200TB dat.	ANO	200 TB - model LOGM-XL-200-4H je vybaven příslušným úložištěm chráněným proti výpadku disků RAID 6
Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“.	ANO	Prohlášení dostupné na stránkách výrobce zde: https://logmanager.com/wp-content/uploads/2024/09/ZKB-a-Logmanager.pdf

Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Průměrný trvalý příjem min. 10000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení Výkon v EPS = 10.000 -maximální udržitelný výkon měřený vudálostech za sekundu (EPS) pro jednotku Logmanageru-XL (Max Constant EPS). Směs surových logů s průměrnou velikostí 700 bajtů, testováno s plným parsováním. Peak EPS se rovná dvojnásobku Max Constant EPS po dobu 10 minut.
Špičkový příjem minimálně 20000 událostí/s po dobu nejméně 5 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení Peak EPS se rovná dvojnásobku Max Constant EPS po dobu 10 minut = 20.000.
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 500GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 200 TB a nad to musí podporovat kompresi ukládaných dat.	ANO	Licencování - Všechny verze Logamangeru (vč. nabízené verze Logmanager-XL) zahrnují neomezený početagentů, zdrojů a systémových uživatelů.
Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z Windows, zpráva byla vygenerována firewallem atd…	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních Windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Předložte kompletní dokumentaci k instalaci a konfiguraci agenta pro sběr logů z prostředí Windows.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení

Podpora sběru z OpenSource Elastic Search Beats (minimálně pro winlogbeat, filebeat).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně Windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Počet instalací Windows agenta nesmí být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 5 000 licencí na dobu předpokládané morální životnosti produktu – 7 let.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení Licencování - Všechny verze logmanageru (vč. nabízené varinaty Logmanager-XL) zahrnují neomezený počet agentů, zdrojů a systémových uživatelů.

Technické požadavky zadavatele na Log forwardery do vzdálených lokalit	**Nabízené řešení splňuje ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Výrobce a model nabízeného produktu:		Logmanager
P/N a další specifikace nabízeného produktu:		LOGM-FW-HW Logmanager-HF
Typ - HW Appliance včetně napájecích kabelů	ANO	HW appliace ve formě MicroPC platform Napájecí zdroj a kabeláž je součástí nabídky
Připojení do LAN - pomocí fyzických portů GE RJ45	ANO	HW appliance je vybavena příslušnými metalickými LAN ethernet porty
Metalický kabel RJ45 min. CAT6 délky 5m jako součást dodávky	ANO	Metalický patchcord je součástí nabídky
Celkový počet zalicencovaných zařízení pro sběr logů - min. 10 000 zařízení	ANO	Více jak 10.000
Počet logů za vteřinu trvale - min. 5 000 logů za vteřinu	ANO	Více jak 9.000 EPS - Maximální udržitelný výkon měřený v událostech za sekundu (EPS) pro jednotku Logmanageru (Max Constant EPS). Směs surových logů s průměrnou velikostí 700 bajtů, testováno s plným parsováním.
Počet logů za vteřinu ve špičce (po dobu min 5 minut) - min. 15 000 logů za vteřinu	ANO	Více jak 18.000 EPS - Peak EPS se rovná dvojnásobku Max Constant EPS po dobu 10 minut.
Celkový objem uložených logů - min. 250GB	ANO	250 GB - model LOGM-FW-HW je vybaven příslušným úložištěm (bufferem)
Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 250GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO	250 GB - model LOGM-FW-HW je vybaven příslušným úložištěm (bufferem)
Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení
Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO	Jedná se o standardní funkční vlastnost nabízeného řešení

Role - Projektový manažer / Team Leader	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Certifikace v oblasti IT service managementu, minimálně ITILv3 Foundation či jiná obdobná či vyšší	ANO	Projektový manažer účastníka, kterým účastník prokazuje technickou kvalifikaci a který se bude podílet na plnění zakázky, je držitelem příslušné certifikace ITILv3 Foundation od roku 2012
Certifikace projektovému managementu, minimálně Prince2 Foundation či jiná obdobná či vyšší	ANO	Projektový manažer účastníka, kterým účastník prokazuje technickou kvalifikaci a který se bude podílet na plnění zakázky, je držitelem příslušné certifikace Prince2 Foundation od roku 2018
Komunikační jazyk: znalost českého nebo slovenského jazyka na minimální úrovni certifikace B2 nebo rodilý mluvčí	ANO	Projektový manažer účastníka, kterým účastník prokazuje technickou kvalifikaci a který se bude podílet na plnění zakázky, je rodilým mluvčím (čeština)
Minimálně 5 let praxe v oblasti řízení implementačních ICT projektů	ANO	Projektový manažer účastníka, kterým účastník prokazuje technickou kvalifikaci a který se bude podílet na plnění zakázky, má praxi v oblasti řízení implementačních ICT projektů v roli projektového managera více jak 10 let

Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	Projektový manažer účastníka, kterým účastník prokazuje technickou kvalifikaci a který se bude podílet na plnění zakázky, je zaměstnancem účastníka, tj. existuje pracovně-právní vztah mezi pracovníkem a účastníkem

Role - Technik pro dodávané řešení Log Managementu	**Splnění ANO/NE**	**Komentář ke způsobu plnění požadavku (pokud je relevantní)**
Certifikace od výrobce nabízeného log managementu řešení na úrovni expertní znalosti nabízeného systému opravňující pracovníka k implementaci takového řešení a integraci do prostředí Zadavatele	ANO	Techničtí specialisté účastníka, kterými účastník prokazuje technickou kvalifikaci a kteří se budou podílet na plnění zakázky, jsou držiteli technické certifikace Logmanager System Expert od výrobce Logmanager (v jednom případě od 2021/09, v druhém případě od 2024/04)
Komunikační jazyk: znalost českého nebo slovenského jazyka na minimální úrovni certifikace B2 nebo rodilý mluvčí	ANO	Techničtí specialisté účastníka, kterými účastník prokazuje technickou kvalifikaci a kteří se budou podílet na plnění zakázky, jsou rodilými mluvčími (v jednom případě se jedná o češtinu, v druhém případě o slovenštinu)
Minimálně 5 let praxe v oblasti implementace informačních či komunikačních technologií ICT	ANO	Techničtí specialisté účastníka, kterými účastník prokazuje technickou kvalifikaci a kteří se budou podílet na plnění zakázky, mají praxi v oblasti implementace ICT více jak 10 let
Existence pracovního nebo obdobného poměru u dodavatele, příp. poddodavatele, nebo, je-li fyzickou osobou podnikající, smluvního vztahu s dodavatelem	ANO	Techničtí specialisté účastníka, kterými účastník prokazuje technickou kvalifikaci a kteří se budou podílet na plnění zakázky, jsou zaměstnanci účastníka, tj. existuje pracovně-právní vztah mezi pracovníky a účastníkem

Minimální seznam podporovaných zdrojů logů

Podporované zdroje logů	Splnění ANO/NE
Apache httpd	ANO
Cisco IOS	ANO
Cisco ISE	ANO
Cisco PRIME	ANO
Cisco WLC	ANO
FlowMon	ANO
FortiADC	ANO
FortiAuthenticator	ANO
FortiDDoS	ANO
Fortigate	ANO
FortiMail	ANO
FortiManager	ANO
FortiSandbox	ANO
FortiWeb	ANO
Helios Green ERP Systém	ANO
HPE iLo (Server OoB management)	ANO
HPE IMC	ANO
Huawei aktivní prvky	ANO
Huawei dohledový systém eSight	ANO
IDM - Identity management systém	ANO
Integrační platforma (ESB a WSO2)	ANO
Linux Bash commands log	ANO
Linux Cron	ANO
Microsoft Active Directory	ANO
Microsoft DHCP servery	ANO
Microsoft DNS servery	ANO
Microsoft Radius servery	ANO
Microsoft SQL	ANO
Microsoft Windows DHCP log	ANO
Microsoft Windows DNS debug log	ANO
Microsoft Windows Firewall	ANO
Microsoft Windows IIS/ftpserver	ANO
Microsoft Windows IIS/webserver	ANO
Microsoft Windows logy z Event View (libovolný adresář)	ANO
Microsoft Windows logy z libovolného textového souboru	ANO
Monitoring - Zabbix, Nagios	ANO
MySQL	ANO
NTP servery	ANO
Objektová Storage DELL ECS	ANO
OpenSSH server	ANO
Red Hat Enterprise Linux	ANO
RFC5425 (generický/standardizovaný formát)	ANO
VEEAM Backup and Restore	ANO
VMware	ANO

Jednotkový ceník

Položka	Jednotka	Cena v Kč bez DPH
Centrální část řešení pro log management včetně záruky a podpory systému ze strany výrobce řešení v režimu 8x5xNBD na období 5 let	kpl	[redacted]
Log forwarder do vzdálených lokalit Zadavatele, včetně fyzické instalace a integrace do Centrálních komponent log managementu, a to včetně rozšířené záruky a podpory systému ze strany výrobce řešení v režimu 8x5xNBD na období 5 let	kpl	[redacted]
Poskytnutí konzultační a implementační podpory pro implementované log management řešení	MD	[redacted]

Předpokládaný model čerpání

Položka	Počet	Jednotka	Cena v Kč bez DPH	Cena celkem v Kč bez DPH
Centrální část řešení pro log management včetně záruky a podpory systému ze strany výrobce řešení v režimu 8x5xNBD na období 5 let	2	kpl	[redacted]	[redacted]
Log forwarder do vzdálených lokalit Zadavatele, včetně fyzické instalace a integrace do Centrálních komponent log managementu, a to včetně rozšířené záruky a podpory systému ze strany výrobce řešení v režimu 8x5xNBD na období 5 let	30	kpl	[redacted]	[redacted]
Poskytnutí konzultační a implementační podpory pro implementované log management řešení	17	MD	[redacted]	[redacted]
CELKEM				**10 979 000,00 Kč**

Digitálně podepsal: [redacted]
Datum: 30.01.2025 13:04:23 +01:00

[redacted]
Digitally signed by [redacted]
Date: 2025.01.28 17:34:22 +01'00'