NEMOCNICE PÍSEK

Kupní smlouva

uzavřená dle ust. § 2079 a násl. zák. č. 89/2012 Sb., občanského zákoníku

Nemocnice Písek, a.s.

společnost zapsaná v obchodním rejstříku vedeném Krajským soudem v Českých Budějovicích pod sp. zn. B 1462

se sídlem:	Karla Čapka 589, 397 01 Písek
IČ:	260 95 190
DIČ:	CZ699005400
jednající:	MUDr. Jiřím Holanem, MBA, předsedou představenstva
	a Ing. Danou Čagánkovou, členem představenstva
číslo účtu:	20830271/0100

na straně jedné (dále jen „**Kupující**")

a

STAPRO s.r.o.

společnost zapsaná v obchodním rejstříku vedeném u KS Hradec Králové, Oddíl C, spisová vložka č. 148

se sídlem:	Pernštýnské nám. 51, 530 02 Pardubice
IČ:	13583531
DIČ:	CZ699004728
jednající:	Ing. Leoš Raibr, jednatel společnosti
číslo účtu:	[redacted]

na straně druhé (dále jen „**Prodávající**")

Prodávající a Kupující dále také jako „**smluvní strany**"

nebo jednotlivě jako „**smluvní strana**"

tímto uzavírají tuto kupní smlouvu v souladu s ustanovením § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném a účinném znění (dále jen „**občanský zákoník**"), jako výsledek výběrového řízení „Úložiště logů" (dále jen „**veřejná zakázka**") zadávaného mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „**ZVZ**").

NEMOCNICE PÍSEK

I. Předmět smlouvy

1. Předmětem této smlouvy je závazek Prodávajícího dodat Kupujícímu úložiště logů dle technické specifikace uvedené v Příloze č. 1 této smlouvy se všemi sjednanými, jinak obvyklými součástmi a příslušenstvím (dále jen „**Zařízení**") a umožnit Kupujícímu k němu nabýt vlastnické právo. Zařízení musí splňovat veškeré požadavky stanované pro jeho uvedení na trh a do provozu dle platných právních předpisů zejména zákona č. 22/1997 Sb., o technických požadavcích na výrobky.
2. Prodávající prohlašuje, že Zařízení je nové, nepoužité, nerepasované, nepoškozené, plně funkční, v nejvyšší jakosti poskytované výrobcem Zařízení a spolu se všemi právy nutnými k jeho řádnému a nerušenému nakládání a užívání Kupujícím.
3. Prodávající prohlašuje, že předmět plnění dle této smlouvy je zcela v souladu s požadavky Kupujícího uvedenými v zadávací dokumentaci veřejné zakázky a že je výlučným vlastníkem Zařízení, že na Zařízení neváznou žádná práva třetích osob a že není dána žádná překážka, která by mu bránila se Zařízením podle této smlouvy disponovat. Prodávající prohlašuje, že Zařízení nemá žádné vady, které by bránily jeho použití ke sjednaným či obvyklým účelům.
4. Kupující se zavazuje Zařízení převzít a zaplatit Prodávajícímu níže uvedenou kupní cenu.

II. Kupní cena

1. Kupní cena za splnění této smlouvy Prodávajícím je sjednána v souladu s cenou, kterou Prodávající nabídl v rámci výběrového řízení na veřejnou zakázku.
2. Kupní cena činí 1 282 378 Kč bez DPH. DPH činí 21% Kč. Kupní cena vč. DPH činí 1 551 677,38 Kč.
3. Kupní cena je sjednána jako závazná a nejvýše přípustná.
4. V kupní ceně jsou zahrnuty veškeré náklady Prodávajícího nezbytné pro řádné a včasné splnění celého předmětu této smlouvy, a to zejména clo, doprava do místa určení, instalace, uvedení do provozu, likvidace odpadu a obalů, instruktáž příslušných zaměstnanců, tj. techniků Kupujícího a obsluhujícího personálu, potřebné doklady ke zboží, vstupní validace a záruční servis. To vše po dobu záruky bez povinnosti Kupujícího platit Prodávajícímu nad rámec sjednané kupní ceny.

III. Platební podmínky

1. Kupující se zavazuje zaplatit Prodávajícímu kupní cenu bezhotovostním převodem na bankovní účet Prodávajícího uvedený v této smlouvě na základě faktury vystavené Prodávajícím po protokolárním bezvadném předání a převzetí Zařízení. Splatnost faktury činí **30 dnů** od jejího vystavení.
2. Prodávající se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
3. V případě, že faktura nebude obsahovat odpovídající náležitosti, je Kupující oprávněn zaslat ji ve lhůtě splatnosti zpět Prodávajícímu k doplnění, aniž se tak dostane do prodlení se splatností. Důvody vrácení sdělí Kupující Prodávajícímu písemně zároveň s vráceným daňovým dokladem. V závislosti na povaze závady je Prodávající povinen daňový doklad včetně jeho příloh opravit nebo

vyhotovit nový. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

4. Přílohu faktury tvoří dodací list.
5. Kupující nebude poskytovat Prodávajícímu zálohy.

IV. Termín plnění

1. Prodávající se zavazuje dodat Zařízení dle podmínek sjednaných v čl. V. této smlouvy nejpozději do **5 týdnů od uzavření kupní smlouvy**.

V. Místo a předání plnění

1. Místem plnění je sídlo Kupujícího.
2. Prodávající bude předem informovat Kupujícího o přesném termínu předání Zařízení nejméně 5 kalendářních dnů před dodáním Zařízení.
3. Kontaktní osobou a odpovědným zaměstnancem Kupujícího je pro účely této smlouvy určen [redacted]
4. Kontaktní osobou Prodávajícího je pro účely této smlouvy určen/a [redacted]
5. Prodávající je povinen sdělit Kupujícímu, které vybavení je nutné pro instalaci mít připravené v místě dodání Zařízení a jaký způsob součinnosti od Kupujícího očekává k úspěšné instalaci Zařízení a instruktáži příslušných osob.
6. Kupující se zavazuje poskytnout potřebnou součinnost při instalaci a instruktáži dle pokynů Prodávajícího. Nemožnost provést instalaci z důvodů nedostatečné připravenosti pracoviště Kupujícím má za následek prodloužení doby plnění uvedené v čl. IV. této smlouvy na dobu nezbytnou k vyřešení všech nedostatků.
7. Dodávka se považuje podle této smlouvy za splněnou, pokud:
   - Zařízení bylo řádně předáno včetně příslušné dokumentace,
   - Zařízení bylo nainstalováno, uvedeno do provozu, byla provedena vstupní validace,
   - byla provedena instruktáž obsluhy, tj. techniků Kupujícího a obsluhujícího personálu,
   - Zařízení bylo řádně předáno bez vad a převzato způsobem sjednaným níže.
8. Vlastnické právo k Zařízení přechází z Prodávajícího na Kupujícího okamžikem převzetí Zařízení Kupujícím. Kupující není povinen převzít Zařízení či jeho část, která je poškozena nebo která jinak nesplňuje podmínky dle této smlouvy.
9. O dodání Zařízení se smluvní strany zavazují sepsat předávací protokol, který podepíší a opatří otisky razítek zástupci obou smluvních stran. Takto opatřený předávací protokol slouží jako doklad o řádném předání a převzetí Zařízení.

VI. Záruční podmínky

1. Prodávající poskytuje Kupujícímu záruku za jakost Zařízení spočívající v tom, že Zařízení, jakož i jeho veškeré části i jednotlivé komponenty, bude po záruční dobu způsobilé pro použití k ujednaným, případně jinak obvyklým účelům a zachová si ujednané, případně jinak obvyklé vlastnosti.
2. Záruční doba se sjednává v délce 60 měsíců od protokolárního bezvadného předání a převzetí Zařízení v případě HW a 12 měsíců od protokolárního bezvadného předání a převzetí Zařízení v případě SW.
3. Záruční servis bude Prodávající provádět bezplatně. Vady musí Kupující uplatnit u Prodávajícího bez zbytečného odkladu poté, co se o nich dozví.
4. V případě výskytu záruční vady je Prodávající povinen zajistit realizaci záručního servisu následující pracovní den po nahlášení vady Kupujícím, a to v místě instalace či umístění Zařízení, zjistit příčinu této vady a v co nejkratším termínu ji bezplatně odstranit.
5. Kupující má právo na úhradu nutných nákladů, které mu vznikly v souvislosti s uplatněním práv z vad.
6. Za záruční vady nebudou považovány ty vady, které byly způsobeny nesprávnou obsluhou nebo údržbou Zařízení nebo úmyslným poškozením Zařízení Kupujícím nebo nepovolanou osobou, případně jakýmikoli jinými zásahy, jednáními nebo skutečnostmi nastalými na straně Kupujícího. Odstranění takto zjištěných vad bude provedeno za úplatu.
7. Je-li vadné plnění podstatným porušením této smlouvy, má Kupující právo na odstranění vady dodáním nového Zařízení bez vady, na odstranění vady opravou Zařízení, na přiměřenou slevu nebo na odstoupení od této smlouvy.
8. Práva Kupujícího z vadného plnění tím nejsou dotčena a řídí se dle ust. § 2099 občanského zákoníku.

VII. Odstoupení od smlouvy

1. Kterákoliv smluvní strana může od této smlouvy odstoupit, pokud zjistí podstatné porušení této smlouvy druhou smluvní stranou.
2. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého smluvní strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít; zejména:
   - prodlení s úhradou kupní ceny nebo její části delším 60 kalendářních dnů;
   - prodlení Prodávajícího s dodáním předmětu plnění dle této smlouvy delším než 60 kalendářních dnů;
   - Zařízení nebude možné Kupujícím během záruční doby užívat po dobu delší 60 kalendářních dnů;
   - jestliže Prodávající ujistil Kupujícího, že Zařízení má určité vlastnosti, zejména vlastnosti Kupujícím výslovně vymíněné, anebo že nemá žádné vady, a toto ujištění se následně ukáže nepravdivým;

- nemožnost odstranění vady dodaného Zařízení; nebo
- v případě, že se kterékoliv prohlášení Prodávajícího uvedené v této smlouvě ukáže jako nepravdivé.

3. Odstoupení od této kupní smlouvy musí mít písemnou formu, musí v něm být přesně popsán důvod odstoupení, podpis odstupující smluvní strany, jinak je odstoupení od této kupní smlouvy neplatné. Tato smlouva zaniká ke dni doručení oznámení odstupující smluvní strany o odstoupení druhé smluvní straně.
4. Odstoupení od této smlouvy se nedotýká práva na náhradu škody vzniklého z porušení smluvní povinnosti a práva na zaplacení smluvní pokuty, ani ujednání o způsobu řešení sporů a volbě práva.

VIII. Odpovědnost za škodu

1. Prodávající je povinen nahradit Kupujícímu v plné výši újmu, která Kupujícímu vznikla vadným plněním nebo jako důsledek porušení povinností a závazků Prodávajícího dle této smlouvy.
2. Prodávající uhradí Kupujícímu náklady vzniklé při uplatňování práv z odpovědnosti za vady.
3. Nebezpečí škody na předmětu plnění přechází na Kupujícího předáním a převzetím Zařízení Kupujícímu.

IX. Sankce

1. Pro případ prodlení Prodávajícího s termínem plnění uvedeným v článku IV. této smlouvy, se Prodávající zavazuje uhradit Kupujícímu smluvní pokutu ve výši 0,5 % z kupní ceny včetně DPH uvedené v čl. II této smlouvy, a to za každý i započatý den prodlení.
2. Uplatněním práv z vad či uplatněním smluvních pokut není dotčeno právo na náhradu újmy v plné výši. Smluvní pokutu je Kupující oprávněn započíst oproti pohledávce Prodávajícího.
3. Pro případ prodlení Kupujícího s úhradou kupní ceny uvedenou v článku II. této smlouvy, se Kupující zavazuje uhradit Prodávajícímu smluvní pokutu ve výši 0,5 % z kupní ceny včetně DPH, a to za každý i započatý den prodlení.
4. Smluvní pokuta je splatná do 30 dnů ode dne doručení výzvy k jejímu zaplacení.

X. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti okamžikem jejího podpisu poslední smluvní stranou. Účinnosti smlouva nabývá dnem uveřejnění v registru smluv dle zákona č. 340/2016 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.
2. Smluvní strany se zavazují, že budou respektovat oprávněné zájmy druhé smluvní strany, budou jednat v souladu s účelem této smlouvy a nebudou jej mařit, přičemž uskuteční veškerá právní a jiná jednání, která se ukáží být nezbytná pro dosažení účelu této smlouvy.

NEMOCNICE PÍSEK

3. Plněním této smlouvy nebude Kupující určen významným dodavatelem či provozovatelem Prodávajícího dle § 8 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.
4. Smluvní strany prohlašují, že údaje uvedené ve smlouvě a taktéž v oprávnění k podnikání jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení druhé smluvní straně. Smluvní strany dále prohlašují, že osoby podepisující smlouvu jsou k tomuto úkonu oprávněny.
5. Tato smlouva je uzavřena podle práva České republiky. Ve věcech výslovně neupravených touto smlouvou se smluvní vztah řídí občanským zákoníkem.
6. Smluvní stranou povinnou zveřejnit smlouvu dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv je Kupující.
7. Pokud některé z ustanovení této smlouvy je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost smlouvy jako celku ani jiných ustanovení této smlouvy, pokud je takovéto neplatné, neúčinné či zdánlivé ustanovení oddělitelné od zbytku této smlouvy. Smluvní strany se zavazují takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejvěrněji odpovídat podstatě a smyslu původního ustanovení.
8. Změna nebo doplnění smlouvy může být uskutečněna pouze písemným dodatkem k této smlouvě podepsaným oběma smluvními stranami.
9. Tato smlouva je vyhotovena ve dvou vyhotoveních, z nichž každá smluvní strana obdrží po jednom vyhotovení.
10. Nedílnou součástí této smlouvy je příloha:

- **Příloha č. 1- Technická specifikace předmětu plnění**

V Písku dne 27. 11. 2023

V Pardubicích dne 21. 11. 2023

KUPUJÍCÍ:

[redacted]

MUDr. Jiří Holan, MBA
předseda představenstva
Nemocnice Písek, a.s.

[redacted]

Ing. Dana Čagánková
člen představenstva
Nemocnice Písek, a.s.

PRODÁVAJÍCÍ:

STAPRO s. r. o.

[redacted]

Ing. Leoš Raibr
Jednatel společnosti
STAPRO s.r.o.

[redacted]

NEMOCNICE PÍSEK

Příloha č. 1 Technická specifikace předmětu plnení

1. Popis požadovaného řešení.

Zadavatel aktuálně provozuje systém Logmanager, který dosud naplňoval požadavky IT provozu a plnil rovněž zásadní právní normy a doporučení pro organizace v rámci IT bezpečnosti pro sběr a ukládání logů. S ohledem na vyšší nároky zadavatele na tento systém, končící životní cyklus stávajícího zařízení a končící SW podporu výrobce, je předmětem této veřejné zakázky výkonový a generační upgrade této HW appliance. Součástí zakázky je také migrace uložených logů za starého zařízení na nové, jakož i převod všech konfigurací, při současném a kompletním zachování konektivit všech logovaných systémů, zařízení a dalších aplikací do tohoto centrálního bezpečnostního prvku, bez nutnosti dalších časových a investičních nákladů do nových konfiguračních prací.

Cílem této veřejné zakázky je pokračování stávajícího řešení na takové, které bude na další období minimálně 5 let, standartně hw 5 let, 3 roky sw položku naplňovat potřeby zadavatele s dostatečnou výkonovou rezervou, bude mít minimálně dvojnásobnou retenční hodnotu uložených dat oproti stávajícímu řešení a bude splňovat současné nároky na kyberbezpečnost jak z hlediska zabezpečení uložených dat, především pak požadavek na zabezpečení obsahu dat proti přepsání, smazání nebo modifikaci pořízených dat, tak i z hlediska norem jako jsou například ZKB/VKB, GDPR a doporučení a standardů jako jsou třeba „Doporučení pro administrátory" od NUKIB, ISO 27001, PCI-DSS a dalších.

Obecný popis požadavků

Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně 18 měsíců zpět. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

Nutností je možnost procházení těchto logů integrovaným grafickým rozhraním s předdefinovanými pravidly pro rychlé vyhledávání, např.:

- změny v systémech provedené administrátory;
- seznam nově vytvořených účtů v MS AD a Office365 za zvolenou periodu;
- změny v přístupových právech pro zadaného uživatele nebo k zadané složce;
- monitoring privilegovaných účtů, sdílených účtů a změn konfigurací;
- sledování souborových systémů apod.

Dále musí systém umožňovat sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

Cílem je mít jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Systém musí dále umožňovat tvorbu uživatelsky definovaných parserů, upozornění a korelací bez účasti výrobce nebo dodavatele ve

snadno pochopitelném grafickém rozhraní bez nutnosti používat znalosti programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.

Nezbytnou nutností je, aby dodaný systém umožňoval zálohování konfigurace i dat a jejich následnou obnovu. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný systém podporoval plánované i ad-hoc zálohování vzniklých dat na externí zálohovací systém, optimálně za využití SMB protokolu. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců – dle "Bezpečnostního doporučení NCKB pro Administrátory 2.0". Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat.

Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Ne všichni naši administrátoři a budoucí operátoři systému dokonale ovládají angličtinu, nebo jiný cizí jazyk, proto požadujeme, aby součástí dodávky byla i dokumentace v českém jazyce, obsahem i kvalitou srovnatelná s aktuální dokumentací v angličtině. Proto v rámci odpovědi na výběrové řízení požadujeme předložit kompletní dokumentaci k celému systému a poznámky k vydání (release notes) k systému i všem návazným komponentům. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Dodaný systém plánujeme provozovat vlastními lidskými zdroji, proto by nabízený systém měl umožňovat našim pracovníkům IT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený systém proto musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.

Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

V případě pochybností o vlastnostech nabízeného systému si vyhrazujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek do 2 týdnů od výzvy zadavatele. Dále si vyhrazujeme právo vyžádat kontakty alespoň na 2 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.

2. Podrobná technická specifikace.

Účastník je povinen níže uvedené tabulky s konkrétními požadavky vyplnit (tj. uvést, zda jím nabízené řešení splňuje či nesplňuje v plném rozsahu uvedený požadavek) a tyto tabulky poté učinit součástí nabídky.

Zadavatel vyžaduje, aby nabízené řešení mělo níže požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.

Pokyny k vyplnění tabulky:

NEMOCNICE PÍSEK

Účastník vyplní políčka – název, typové označení a v pravém sloupci tabulky účastník vyplní „Ano", jestliže nabízené řešení splňuje požadované parametry.

Účastník do nabídky rovněž vloží dokumentaci k jednotlivým technickým parametrům dle požadavků zadavatele uvedených v Technické specifikaci (např. produktové listy, katalogové listy, ověřitelný konkrétní www odkaz na dokumenty apod.).

Nesplnění požadovaných parametrů vede k vyřazení nabídky z dalšího posuzování a hodnocení a vyloučení účastníka z výběrového řízení.

Technická specifikace systému pro centralizované ukládání a správu logů		
Popis řešení SEM/SIEM do 5000 událostí/s s minimálně 80TB velikostí databáze		
Název, typové označení	**Logmanager-L, , server Dell** **5 let HW záruka, 3 roky SW renewal, 1x LOGmanager-VF, 40 TB databáze** **Rozšíření diskového prostoru Logmanageru-L o 40 TB (celková kapacita 80 TB)**	
Číslo	**Požadavek**	**Splňuje ANO/NE**
1	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.	ANO
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz seznam podporovaných zařízení v Příloze č. 1 zadávací dokumentace - Priloha_1_Seznam_podporovanych_systemu.xlsx.	ANO
3	Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	ANO
4	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	ANO

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

16	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.	ANO
17	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	ANO
18	Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory. Doložte odkazem na dokumentaci, jakým způsobem se požadované funkce v grafickém rozhraní systému nastavují.	ANO
19	Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.	ANO
20	V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	ANO
21	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).	ANO
22	Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.	ANO
23	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
24	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
25	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO
26	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
27	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. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.	ANO
28	Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO
29	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 80TB dat.	ANO

30	Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO
31	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ANO
32	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. Požadujeme předložit vzorový návod na integraci s externím monitorovacím systémem.	ANO
33	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
34	Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	ANO
35	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.	ANO
36	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
37	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	ANO
	Minimální HW parametry požadovaného systému	
38	Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	ANO
39	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	ANO
40	2 procesory, min. 16 jader každý, s podporou HyperThreadingu nebo Multi-Threadingu.	ANO
41	Min. 128 GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	ANO
42	Minimálně 80 TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 8 GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	ANO
43	Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	ANO

44	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci.	ANO
45	Větráky v systému musí být vyměnitelné za provozu a redundantní.	ANO
46	2x napájecí zdroje s redundancí napájení 1+1.	ANO
47	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	ANO
48	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ANO
	Výkonnostní a SW parametry systému	ANO
49	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	ANO
50	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	ANO
51	Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade.	ANO
52	Průměrný trvalý příjem min. 5000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	ANO
53	Špičkový příjem minimálně 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	ANO
54	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300 GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 80TB a nad to musí podporovat kompresi ukládaných dat.	ANO
55	Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	ANO
56	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a ident. výrobce zařízení podle MAC adresy.	ANO

57	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. Doložte odkazem na dokumentaci, jakým způsobem lze plnit textové tabulky prostřednictvím REST-API nabízeného systému.	ANO
58	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	ANO
59	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, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd.	ANO
60	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
61	Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 2 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.	ANO
62	Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.	ANO
63	V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	ANO
64	Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.	ANO
65	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
66	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí	ANO

	zálohování a obnova konfigurace systému.	
67	Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	ANO
	Alerty	
68	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO
69	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO
70	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO
71	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. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.	ANO
72	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.	ANO
73	V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	ANO
74	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.	ANO
	Sběr událostí z Microsoft prostředí	
75	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.	ANO
76	Agent provádí instalaci a podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému. Doložte odkazem na dokumentaci, jakým způsobem se provádí centralizované řízení a konfigurace Microsoft Sysmon služby.	ANO
77	Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036.	ANO

78	Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.	ANO
79	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.	ANO
80	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířit Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.	ANO
81	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash.	ANO
	Podpora pro sběr událostí	
82	Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	ANO
83	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	ANO
84	Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení rešení pro sběr událostí na pobočkách.	ANO
85	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100 GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO
86	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO
87	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO
88	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO
89	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO
	SW Podpora a záruka na hardware	
90	HW - Požadovaná min. 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	ANO

91	Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO
92	SW - Podpora výrobce na aktualizaci systému a parserů na **3** roky. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO
	Kompletní implementace	
93	Provedení předimplementační analýzy a návrhu řešení	ANO
94	Zaškolení správců systému	ANO
95	Akceptační testy	ANO

3. Ostatní podmínky

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
Účastník je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

4. Napojení logování z technologických systémů

Dodavatel zrealizuje ukládání logů do dodaného systému z těchto zařízení:

Číslo	Počet ks	Popis
1	40	Windows servery
2	600	Windows desktopy
3	10	Linux servery
4	5	Virtualizace Vmware
7	40	Ethernetové switche HPE/Aruba
8	1	Wifi kontrolér Aruba
9	2	Firewall, IPS, VPN, WAF, antivir, webfiltr
10	1	Flowmon
11	2	Web servery IIS
12	2	Databáze MS SQL
13	1	Mail server
14	1	Management serverů (HPE iLO, iDrac apod.)

5. Předpokládaná součinnost ze strany zadavatele

Přístup do prostor zadavatele
Součinnost správců IT technologií včetně přístupových údajů k dotčeným systémům (servisní účty)
Vzdálený přístup pro specialistu – VPN
Poskytnutí kontaktů

6. Minimální seznam podporovaných zdrojů logů

AIP Safe (https://aipsafe.cz/)
Apache httpd
Apache Tomcat
Amavis
Antivir AVG
Antivir Avast
Antivir Eset Remote administrator
Brocade FC switches
ArcSight CEF (generický/standardizovaný formát)
Barracuda Email Security Gateway
Cisco ASA
Cisco ASA-Lite (optimalizované pro výkon)
Cisco Firepower
Cisco ISE
Cisco IOS
Cisco IronPort
Cisco Nexus
Cisco SMB
Cisco UCS
Cisco WLC
CompuNet GAMA
Dell Force10
Dell iDrac
Dell Isilon
Dell PowerConnect
Dell SonicWALL
Dell W-series WiFi
Discard (speciální pravidlo na fitrování událostí)
Dropbear SSH (~součást Embedded Linux distribucí)
Epacs (http://www.epacs.cz/)
Extreme NAC
Extreme Networks XOS
Flowmon
FortiAuthenticator
FortiDDoS
Fortigate
FortiGate-Lite (optimalizované pro výkon)
FortiMail
FortiManager
FortiADC
FortiSandbox

FortiWeb
F5 BigIP ASM
FreeRADIUS
Greycortex NTA
Qradar LEEF (generický/standardizovaný formát)
H3C networking
HAProxy (structured rfc5425 logformat)
Hillstone NGFW
HPE Aruba Instant AP (WLAN)
HPE Aruba Clearpass
HPE Aruba Mobility Controller (WLAN)
HPE iLo (Server OoB management)
HPE IMC
HPE routers
HPE switches Aruba OS
HPE switches Aruba-CX OS
HPE switches Comware OS
HPE Comware WLAN
Huawei USG
IceWarp
CheckPoint LOG Exporter Lite (optimalizován na výkon)
CheckPoint LOG Exporter
ISC BIND
ISC DHCP
Jivex
JSON (generický/standardizovaný formát)
Juniper SRX
Juniper SRX-Lite (optimalizované pro výkon)
Kaspersky Endpoint Security
Kaspersky Security Center
Kemp LoadMaster
Kerio Connect
Kerio Control
Kernun Clear Web
Kernun Web filter
Lenovo XClarity (Server OoB management)
Linux Bash commands log
Linux Cron
Linux Freeradius
Linux Iptables
Linux Postfix
Mikrotik
Microsoft365 (API)

Microsoft Azure (API)
Microsoft Exchange
Microsoft Exchange tracking textový log (2010-2019)
Microsoft SharePoint
Microsoft SQL
Microsoft Windows Defender
Microsoft Windows DHCP textový log
Microsoft Windows DNS debug textový log
Microsoft Windows Firewall (EVTx i textový log)
Microsoft Windows IIS / FTP server textový log
Microsoft Windows IIS / Webserver textový log
Microsoft Windows logy z Event View (libovolný EVTx adresář)
Microsoft Windows logy z libovolného textového souboru
Microsoft Windows Sysmon
MySQL
Nginx
Novell eDirectory
Office365
OpenSSH server
Oracle DB
Palo Alto Networks NGFW
PostgreSQL
Pulse Secure
Qnap
Ruckuss wireless
Safetica DLP
SAP (SM19 a SM20 logy)
Shorewall
Siemens Scalance
SonicWall
Sophos
SpamAssasin
Stapro FONS Enterprise, Akord, Openlims
Squid (Web Proxy)
Squid for Windows
Radware Defense Pro
RFC5425 (generický/standardizovaný formát)
Symantec Endpoint Protection Manager
Symantec Messaging Gateway (Brightmail)
Synology NAS DSM
Trapeze
Trend Micro Apex One
TrendMicro DeepDiscovery

TrendMicro DeepSecurity
TrendMicro TippingPoint SMS
UBNT Rocket
UBNT UniFI
Vectra Contigo
VEEAM Backup and Restore
Vmware vCenter a ESXi
Vmware Horizon
Whalebone.io (DNS server)
Zimbra
Zyxel