[redacted]

2021/0896/[redacted]

KUPNÍ SMLOUVA

uzavřená dle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění
(dále jen „smlouva")

Dodávka systému pro záznam událostí

[redacted]

Statutární město Kladno

se sídlem:	náměstí Starosty Pavla 44, 272 52 Kladno
zastoupené ve věcech smluvních:	Ing. Přemyslem Mužíkem, náměstkem primátora
zastoupené ve věcech technických:	Bc. Petrem Jorgem, pověřeným vedoucím oddělení ICT
IČ:	00234516
DIČ:	CZ00234516

(dále jen jako „kupující")

a

CompuNet s.r.o.

zapsaný:	v OR u MS v Praze, oddíl C, vložka 118594
se sídlem:	Zubatého 295/5, 150 00 Praha 5
zastoupený ve věcech smluvních:	[redacted] jednatelem
ve věcech technických:	[redacted]
IČ:	276 08 514
DIČ:	CZ 276 08 514
bankovní spojení:	Komerční banka a.s.
č. ú.:	[redacted]
Kontaktní osoba:	Martin Pokorný
Email:	[redacted]
Telefon:	[redacted]

(dále jen „prodávající")
(společně také jako „smluvní strany" nebo každý samostatně jako „smluvní strana")

Preambule

Tuto smlouvu uzavírá kupující jako zadavatel veřejné zakázky malého rozsahu na dodávky s názvem „Dodávka systému pro záznam událostí" (dále jen „veřejná zakázka") s prodávajícím jako vybraným dodavatelem ve věci předmětné veřejné zakázky. Zadávací dokumentace k výše uvedené veřejné zakázce, včetně podle ní prodávajícím doložených příloh a nabídky, logicky doplňuje smlouvu a je nepostradatelnou pomůckou zejména v případě pochybností při výkladu jednotlivých ustanovení smlouvy. Prodávající tak výslovně prohlašuje, že respektuje veškeré zadávací podmínky kupujícího stanovené v zadávací dokumentaci veřejné zakázky a nečiní k nim žádné výhrady.

[redacted]

I. Předmět smlouvy

1. Prodávající se touto smlouvou zavazuje, že kupujícímu odevzdá předmět koupě popsaný v příloze č. 1 smlouvy (dále jen „Předmět koupě") a umožní nabýt kupujícímu k Předmětu koupě vlastnické právo, a kupující se zavazuje, že Předmět koupě převezme a zaplatí prodávajícímu kupní cenu dle čl. III. smlouvy.

2. Technická specifikace Předmětu koupě je uvedena v příloze č. 1 této smlouvy, která je její nedílnou součástí a obsahově odpovídá technické specifikaci předmětu koupě, kterou prodávající vložil do jeho nabídky podané v rámci veřejné zakázky.

II. Místo a doba plnění

1. Místem odevzdání Předmětu koupě je sídlo kupujícího.

2. Prodávající se zavazuje odevzdat kupujícímu Předmět koupě na vlastní náklady nejpozději do 60 dnů ode dne nabytí účinnosti smlouvy.

3. Smluvní strany se dohodly, že prodávající je oprávněn dodat Předmětu koupě; v úplnosti však musí být celý Předmět koupě dodán kupujícímu nejpozději ve lhůtě uvedené v odst. 2 tohoto článku, tj. do 60 dnů ode dne účinnosti této smlouvy.

4. Prodávající se zavazuje předat kupujícímu současně s každou položkou Předmětu koupě veškeré doklady potřebné k převzetí a užívání dodané věci - technické listy, návody k užívání, záruční listy apod.

5. Smluvní strany se dohodly, že o předání Předmětu koupě prodávajícím kupujícímu, a to dílčím předání Předmětu koupě, bude sepsán protokol o převzetí věci ve dvojím vyhotovení a každá smluvní strana obdrží po jednom vyhotovení.

III. Cena a platební podmínky

1. Kupující se zavazuje zaplatit prodávajícímu za **celý Předmět koupě** dle č. I. smlouvy, resp. po jeho řádném předání, sjednanou kupní cenu ve výši 1.967.500,- Kč bez DPH, 413.175,- Kč DPH (21%), 2.380.675,- Kč včetně DPH (dále jen „celková cena").
2. Celková cena je konečná a zahrnuje záruku za jakost a veškeré další náklady prodávajícího související s odevzdáním zboží (např. doprava zboží do místa odevzdání, zabalení zboží).
3. Faktura – daňový doklad vystavený prodávajícím musí obsahovat všechny náležitosti daňového dokladu vč. označení příslušné smlouvy a čísla alokace finančních prostředků kupujícího (dále jen „faktura").
4. Splatnost je stanovena na 30 dnů od data vystavení faktury prodávajícím, a to za předpokladu jejího doručení na fakturační adresu, kterou je sídlo kupujícího, do tří dnů od data vystavení.
5. Nebude-li faktura obsahovat veškeré náležitosti podle zákona č. 235/2004 Sb., o dani z přidané hodnoty v platném znění, nebo podle jiných obecně platných právních předpisů nebo bude-li v rozporu s podmínkami vyúčtování podle smlouvy, je kupující oprávněn fakturu prodávajícímu vrátit s pokyny k její opravě. V takovém případě splatnost faktury nezačala běžet a splatnost nové opravné faktury počne běžet od samého počátku až prvním dnem jejího doručení kupujícímu.

IV. Změny smlouvy a komunikace smluvních stran

1. Tato smlouva může být změněna pouze písemným oboustranně potvrzeným ujednáním nazvaným „dodatek ke smlouvě".

2. Zástupce kupujícího:

   Bc. Petr Jorg, MBA, e-mail:

3. Zástupce prodávajícího:

   Martin Pokorný e-mail:

4. Pokud by některá ze smluvních stran změnila své zástupce pro věcná nebo technická jednání, je povinna písemně vyrozumět druhou smluvní stranu do 5 dnů po takové změně. Řádným doručením tohoto oznámení dojde ke změně zástupce bez nutnosti uzavření dodatku k této smlouvě.

V. Záruka za jakost

1. Prodávající prohlašuje, že dodané zboží, které je Předmětem koupě, je nové, nepoužívané a odpovídá platným právním předpisům, českým technickým normám (ČSN), dokumentaci výrobce ke zboží a má platné prohlášení o shodě. Prodávající prohlašuje, že zboží není zatíženo žádnými právy třetích osob. Prodávající předá kupujícímu veškerou dokumentaci vztahující se k zařízení, která je potřebná pro nakládání s přístrojem a pro jeho provoz, nebo kterou vyžadují příslušné obecně závazné právní předpisy a české a evropské normy ČSN a EN (návod k použití v českém jazyce, technická dokumentace, pokyny pro údržbu, prohlášení o shodě, apod.) bude doručena doporučenou poštou nebo osobně pověřenému zaměstnanci kupujícího proti písemnému potvrzení.

2. Prodávající poskytuje na zboží, které tvoří Předmět koupě záruku za jakost v délce odpovídající požadavkům kupujícího v zadávacích podmínkách veřejné zakázky. Záruční doba počíná běžet okamžikem odevzdáním zboží kupujícímu. Zárukou za jakost se prodávající zavazuje, že zboží bude po dobu odpovídající záruce způsobilé ke svému obvyklému účelu, jeho kvalita bude odpovídat této smlouvě a zachová si vlastnosti touto smlouvou vymezené popř. obvyklé.

3. Součástí dodávky zařízení bude písemné potvrzení výrobce nebo oficiálního distributora pro ČR, že dodávané zboží je nové, že je určeno pro český trh (včetně soupisu výrobních čísel dodaných zařízení) a že záruční servis zajišťuje přímo výrobce zařízení. Záruka a přímá podpora bude registrovaná pro Statutární město Kladno. Porušení tohoto závazku bude považováno za podstatné porušení smluvní povinnosti s právem kupujícího odstoupit od smlouvy.

VI. Práva a povinnosti smluvních stran

1. Kupující je povinen předávat prodávajícímu všechny potřebné informace a údaje, které má kupující a které jsou nutné k tomu, aby prodávající mohl poskytovat plnění.

2. Kupující má právo na úplné a včasné plnění ze strany prodávajícího v souladu s touto smlouvou.

3. Prodávající je povinen při poskytování plnění počínat si s náležitou odbornou péčí, v souladu s obecně závaznými právními předpisy, v souladu s touto smlouvou. Dále je povinen nejednat v rozporu s oprávněnými zájmy kupujícího a zdržet se veškerého jednání, které by mohlo kupujícího jakýmkoliv způsobem poškodit.

4. Prodávající je povinen zajistit, aby všechny osoby podílející se na plnění pro kupujícího, které jsou v pracovním nebo jiném obdobném poměru k prodávajícímu nebo jsou k prodávajícímu ve smluvním vztahu, se řídily vždy touto smlouvou. Poruší-li taková osoba jakékoliv ustanovení této smlouvy, bude se na to hledět, jako by porušení způsobil sám prodávající.

5. Smluvní strany se zavazují poskytovat si navzájem při odstraňování vad zboží veškerou potřebnou součinnost tak, aby byly vady řádně a včas odstraněny. Prodávající je povinen zejm.:

   a) v případě odstranění vady dodáním nového zboží dodat nové zboží na tutéž adresu, kde bylo kupujícímu odevzdáno nahrazované zboží, a

b) převzít zboží, jehož vada má být odstraněna opravou, k opravě v místě, kde bylo kupujícímu odevzdáno, a po provedení opravy opravené zboží opět v tomto místě předat kupujícímu. Převzetí zboží k odstranění vad a následné předání zboží po odstranění vad proběhne vždy v pracovní dny v době od 9:00 do 16:00 hod., nebude-li mezi prodávajícím a kupujícím dohodnuto jinak.

6. Prodávající je povinen v průběhu záruční doby provádět bezplatně veškeré servisní úkony, jejichž provedením podmiňuje platnost záruky. Termíny servisních úkonů budou stanoveny dle provozních možností kupujícího.

7. Reklamované vady se prodávající zavazuje odstranit v souladu s uplatněným právem kupujícího bezodkladně, nejpozději však do 15 dnů ode dne doručení reklamace, a to i v případě, že odstraňování vady provede prodávající třetí osobou.

8. Uplatnění práv z vadného plnění kupujícím, jakož i plnění jim odpovídajících povinností prodávajícího není podmíněno ani jinak spojeno s poskytnutím jakékoli další úplaty kupujícího prodávajícímu, příp. jiné osobě.

VII. Smluvní sankční podmínky

1. Bude - li prodávající v prodlení s odevzdáním zboží nebo s vyřízením reklamace, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 1.000,- Kč bez DPH za každý (i započatý) den prodlení. Smluvní pokutou není dotčen nárok kupujícího na náhradu případné škody.

2. Bude-li kupující v prodlení s úhradou ceny nebo její části, je prodávající oprávněn požadovat na kupujícím úhradu smluvní pokuty ve výši 0,1 % z dlužné částky bez DPH za každý (i započatý) den prodlení.

3. Smluvní pokuty jsou splatné ve lhůtě 15 dnů ode dne odeslání výzvy k úhradě smluvní pokuty.

VIII. Prohlášení smluvních stran

1. Prodávající prohlašuje, že Předmět koupě je nový a bez jakýchkoli vad a poškození.
2. Prodávající prohlašuje, že na Předmětu koupě nebudou k okamžiku dodání váznout žádné závazky, zástavní práva ani jiná práva třetích osob, které by omezovaly výkon vlastnického práva kupujícího.
3. Kupující podle možnosti prohlédne Předmět koupě co nejdříve po přechodu nebezpečí škody na věci a přesvědčí se o jeho vlastnostech a množství.
4. Současně s touto smlouvou smluvní strany uzavírají tzv. Non Disclosure Agreement (NDA), jejíž předmětem je ochrana důvěrných informací a zajištění mlčenlivosti o skutečnostech, které se strany v rámci plnění smlouvy dozví a které jsou předmětem obchodního tajemství.

IX. Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího zveřejnění v registru smluv.

2. Tato smlouva se uzavírá elektronicky, tj. připojením elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, do této Smlouvy a všech jejich případných jednotlivých příloh, nejsou-li součástí

[redacted]

[redacted] jediného elektronického dokumentu (tj. všech samostatných souborů tvořících v souhrnu Smlouvu), Smluvními stranami (poslední z nich).

[redacted]

3. Právní vztahy z této smlouvy vzniklé se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

[redacted]

4. Tato smlouva je vyhotovena ve 4 stejnopisech s platností originálu, z nichž 3 stejnopisy obdrží kupující 1 stejnopis prodávající.

5. Smluvní strany prohlašují, že se seznámily s obsahem této smlouvy, kterou uzavírají na základě své pravé, vážné a svobodné vůli, nikoliv v tísni anebo za nápadně nevýhodných podmínek, což stvrzují svými podpisy.

6. Smluvní strany berou na vědomí, že tato smlouva i následné dodatky k ní mohou podléhat informační povinnosti dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím a v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů, a prohlašují, že žádné ustanovení této smlouvy nepovažují za obchodní tajemství ani za důvěrný údaj a smlouva může být zveřejněna v plném znění včetně jejích příloh a dodatků.

7. Prodávající potvrzuje, že poskytnuté osobní údaje uvedené v této smlouvě jsou přesné a že se jedná o dobrovolné poskytnutí osobních údajů. Kupující je ve smyslu *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)* a zákona č. 110/2019 Sb. o zpracování osobních údajů, správcem osobních údajů subjektů údajů a že zpracovává a shromažďuje osobní údaje prodávajícího za účelem realizace této smlouvy. Kupující se zavazuje zpracovávat osobní údaje prodávajícího pouze k účelu danému touto smlouvou, bez využití jiného zpracovatele údajů. Prodávající prohlašuje, že si je vědom všech svých zákonných práv v souvislosti s poskytnutím svých osobních údajů k účelu danému touto smlouvou. Podrobné informace o ochraně osobních údajů jsou uvedeny na oficiálních webových stránkách www.mestokladno.cz v sekci Ochrana osobních údajů.

8. Nedílnou součástí této smlouvy jsou její přílohy:

   Příloha č. 1 – Technická specifikace Předmětu koupě

9. Na důkaz svého souhlasu s obsahem této smlouvy k ní smluvní strany připojily své elektronické podpisy dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

[redacted]

V Praze dne:……. V Kladně dne …….

Za prodávajícího: Za kupujícího:

Ing
Pav
Pik
…… ……

Statutární město Kladno

Přemysl Mužík

náměstek

[redacted]

Příloha č.1 – Technická specifikace Předmětu koupě

Předmět zakázky:
Navrhnout, dodat a implementovat centrální úložiště pro sběr a analýzu logů (SEM/SIEM řešení) s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, zejména pak doložením souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. 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 jeden rok 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. jako jsou 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 snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalostí programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.

Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný 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 4.0". Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo 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, 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.
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 1

týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále si vyhrazujeme právo vyžádat kontakty alespoň na 3 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.

Systém musí dále umožňovat bezeztrátový sběr a příjem událostí ze zdrojů na pobočkách, a to vlastním řešením. Toto řešení zamezí ztrátě událostí během přenosu po mnohdy saturovaných a ne zcela spolehlivých linkách. Realizace sběru a přenosu událostí z poboček do centrálního úložiště může být realizována jak fyzickým, tak virtuálním řešením. V případě nabídnutí virtuálního řešení požadujeme systém pro platformu VMware ESXi.

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

Číslo	Řešení SEM/SIEM do 10000 událostí/s s minimálně 160TB velikostí databáze	Nabídnutá specifikace (účastník přesně popíše, jak nabízení zařízení plní požadované parametry)
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	
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, SPLŇUJE viz str. 29 a 31
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz tabulka seznam podporovaných zařízení).	ANO, SPLŇUJE
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, SPLŇUJE
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, SPLŇUJE viz str. 29

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, SPLŇUJE VIZ STR. 29
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, SPLŇUJE VIZ STR. 29
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, SPLŇUJE
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, SPLŇUJE
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, SPLŇUJE
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, SPLŇUJE
11	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO, SPLŇUJE
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, SPLŇUJE
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, SPLŇUJE VIZ STR. 29
14	Systém provádí konsolidaci logů na interním storage logovacího systému.	ANO, SPLŇUJE
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, SPLŇUJE VIZ STR. 29
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, SPLŇUJE

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, SPLŇUJE
18	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, SPLŇUJE
19	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, SPLŇUJE viz str. 29
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, SPLŇUJE
21	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	ANO, SPLŇUJE
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, SPLŇUJE viz str. 29 a 33
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, SPLŇUJE
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, SPLŇUJE
25	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO, SPLŇUJE
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, SPLŇUJE
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, SPLŇUJE viz str. 29
28	Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO, SPLŇUJE
29	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně **160TB** dat.	ANO, SPLŇUJE
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, SPLŇUJE
31	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ANO, SPLŇUJE

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 VIZ STR. 29
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, SPLŇUJE VIZ STR. 34
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, SPLŇUJE VIZ STR.
35	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí.	ANO, SPLŇUJE VIZ STR. 29
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, SPLŇUJE
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, SPLŇUJE
	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, SPLŇUJE
39	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	ANO, SPLŇUJE
40	2 procesory, min. 16 jader každý, s podporou HyperThreadingu.	ANO, SPLŇUJE
41	Min. 128GB DDR-4 a NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	ANO, SPLŇUJE
42	Minimálně **160TB** pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 8GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	ANO, SPLŇUJE
43	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, SPLŇUJE VIZ STR. 29
44	Větráky v systému musí být vyměnitelné za provozu a redundantní.	ANO, SPLŇUJE
45	2x napájecí zdroje s redundancí napájení 1+1.	ANO, SPLŇUJE
46	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	ANO, SPLŇUJE
47	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ANO, SPLŇUJE
	Výkonnostní a SW parametry systému	

48	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, SPLŇUJE
49	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, SPLŇUJE VIZ STR. 29 a 35
50	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, SPLŇUJE VIZ STR. 30
51	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, SPLŇUJE
52	Špičkový příjem minimálně 20000 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, SPLŇUJE
53	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 120 TB a nad to musí podporovat kompresi ukládaných dat.	ANO, SPLŇUJE
54	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, SPLŇUJE
55	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, SPLŇUJE
56	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, SPLŇUJE VIZ STR. 30
57	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského	ANO, SPLŇUJE VIZ STR. 30

	parseru a jakým způsobem je prezentován výstup testu.	
58	V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...	ANO, SPLŇUJE
59	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	ANO, SPLŇUJE
60	Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – požadujeme podporu minimálně 2 nodů. 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, SPLŇUJE VIZ STR. 30
61	V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.	ANO, SPLŇUJE
62	V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	ANO, SPLŇUJE
63	Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.	ANO, SPLŇUJE
64	Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	ANO, SPLŇUJE
65	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	ANO, SPLŇUJE VIZ STR. 30
66	Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	ANO, SPLŇUJE VIZ STR. 30
	Alerty	
67	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO, SPLŇUJE
68	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO, SPLŇUJE
69	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO, SPLŇUJE

70	Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace 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, SPLŇUJE VIZ STR. 30
71	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.	ANO, SPLŇUJE VIZ STR. 30
72	V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	ANO, SPLŇUJE VIZ STR. 30
73	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci.	ANO, SPLŇUJE
	Sběr událostí z Microsoft prostředí	
74	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. . Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Předložte kompletní dokumentaci k instalalaci a konfiguraci agenta pro sběr logů z prostředí windows.	ANO, SPLŇUJE VIZ STR. 30
75	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	ANO, SPLŇUJE
76	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.	ANO, SPLŇUJE
77	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. 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, SPLŇUJE VIZ STR. 30
78	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. Doložte odkazem na dokumentaci, jakým způsobem se centrálně z grafického rozhraní spravují Windows agenti včetně všech možností nastavení.	ANO, SPLŇUJE VIZ STR. 30
79	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ANO, SPLŇUJE

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. 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, SPLŇUJE VIZ STR. 30
81	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO, SPLŇUJE
82	Počet instalací Windows agenta by neměl být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 1000 na dobu předpokládané morální životnosti produktu - 7 let. Pokud je dodávaný Windows Agent výrobkem třetí strany, doložte digitálně podepsaný souhlas výrobce software třetí strany s použitím 1000 licencí na dodávaného Windows agenta v naší organizaci po dobu 7 let.	ANO, SPLŇUJE VIZ STR. 30
	Podpora pro sběr událostí z poboček	
83	Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.	ANO, SPLŇUJE VIZ STR. 30
84	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, SPLŇUJE
85	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, SPLŇUJE
86	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO, SPLŇUJE
87	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO, SPLŇUJE
88	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO, SPLŇUJE
89	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO, SPLŇUJE
90	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO, SPLŇUJE
91	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO, SPLŇUJE
	Vysoká dostupnost, SW Podpora a záruka na hardware	
92	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.	ANO, SPLŇUJE
93	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, SPLŇUJE
94	Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO, SPLŇUJE
95	SW - Podpora výrobce na aktualizaci systému a parserů na 2 roky. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO, SPLŇUJE
96	Školení administrátoru pro 5 osob v rozsahu min. 8h	ANO, SPLŇUJE

Tabulka č.1 seznam zdrojů logů

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 (na vyžádání)
Dell Force10
Dell iDrac (Server OoB management)
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
F5 BigIP ASM
FreeRADIUS
Greycortex NTA

Qradar LEEF (generický/standardizovaný formát)
HAProxy (structured rfc5425 logformat)
Hillstone NGFW
HPE Aruba Instant AP (WLAN)
HPE Aruba Mobility Controller (WLAN)
HPE iLo 4 (Server OoB management)
HPE IMC
HPE routers
HPE switches Procurve OS
HPE switches Comware OS
HPE Comware WLAN
Huawei USG
CheckPoint LOG Exporter Lite (optimalizován na výkon)
CheckPoint LOG Exporter
CheckPoint via OPSEC protocol
ISC BIND
ISC DHCP
JSON (generický/standardizovaný formát)
Juniper SRX
Juniper SRX-Lite (optimalizované pro výkon)
Kaspersky Endpoint Security
Kaspersky Security Center
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
LOGmanager
Mikrotik
Microsoft Exchange
Microsoft Exchange tracking log (2010-2019)
Microsoft SharePoint
Microsoft SQL
Microsoft Windows DHCP log
Microsoft Windows DNS debug log
Microsoft Windows Firewall
Microsoft Windows IIS/webserver
Microsoft Windows IIS/ftpserver

Microsoft Windows logy z Event View (libovolný adresář)
Microsoft Windows logy z libovolného textového souboru
Microsoft Windows-lite (optimalizované pro výkon)
MySQL
Nginx
Novell eDirectory
Office365
OpenSSH server
Oracle DB
Palo Alto Networks NGFW
PostgreSQL
Pulse Secure
Ruckuss wireless
Safetica DLP
SAP (SM19 a SM20 logy)
Shorewall
SonicWall
Sophos

SpamAssasin
Stapro FONS Enterprise, Akord, OpenIims
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
VEEAM Backup and Restore
Whalebone.io (DNS server)
Vmware (včetně květnové aktualizace VMWARE 7.0)