Kupní smlouva

uzavřená podle ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník,
ve znění pozdějších předpisů (dále jen „Smlouva“)

1. Smluvní strany

Kupující:	**Ostravská univerzita**
sídlo:	Dvořákova 7, 701 03 Ostrava
zastoupená:	prof. MUDr. Jan Lata, CSc. - rektor Ostravské univerzity
IČ:	61988987
DIČ:	CZ61988987
bankovní spojení:	ČNB Ostrava
č. účtu:	931761/0710

(dále jen „Kupující“ nebo „OU“ nebo „Zadavatel“)

Prodávající:	**CompuNet s. r. o.**
sídlo:	Zubatého 295/5, 150 00 Praha 5
zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl C, vložka 118594	
zastoupená:	Ing. Pavel Pikhart, jednatel
IČ:	276 08 514
DIČ:	CZ27608514
bankovní spojení:	Komerční banka a. s.
č. účtu:	51-1998450287/0100

(dále jen „Prodávající“)

2. Základní ustanovení

2.1. Tato smlouva je uzavřena na základě zadávacího řízení na veřejnou zakázku „OU - Rozvoj a obnova klíčových částí systémů informačních a komunikačních technologií univerzity - Zařízení pro uložení a analýzu logů“.

2.2. Smluvní strany prohlašují, že údaje v článku I. této Smlouvy a taktéž 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 straně. Strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto úkonu oprávněny.

3. Předmět koupě

3.1. Předmětem této smlouvy je dodávka a implementace centrálního úložiště pro sběr a analýzu logů (SEM/SIEM řešení) s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací dle Přílohy č. 1, která je součástí této Smlouvy (dále jen „zboží“). Předmětem této smlouvy je rovněž implementace do stávající sítě.

3.2. Prodávající se zavazuje odevzdat kupujícímu zboží specifikované v Příloze č. 1 této Smlouvy a umožnit kupujícímu nabýt ke zboží vlastnické právo. Kupující se zavazuje zboží převzít a zaplatit prodávajícímu kupní cenu.

3.3. 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.

3.4. 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 Ostravskou univerzitu. Porušení tohoto závazku bude považováno za podstatné porušení smluvní povinnosti s právem kupujícího odstoupit od smlouvy.

3.5. Jakost, provedení, vlastnosti a další specifikace zboží včetně jeho množství jsou uvedeny v Příloze č. 1 Smlouvy.

3.6. Závazek prodávajícího odevzdat zboží zahrnuje také dopravu zboží na místo odevzdání zboží a předání dokladů potřebných k užívání či provozu zboží, návod (návody) k obsluze v českém jazyce, jsou-li nezbytné pro používání zboží, příp. dalších dokladů, které se ke zboží jinak vztahují, včetně atestů, certifikátů, prohlášení o shodě, a dále provedení všech činností souvisejících s dodávkou a dále zaškolení obsluhy.

3.7. Prodávající prohlašuje, že:

3.7.1. je výlučným vlastníkem zboží, které kupujícímu odevzdá,

3.7.2. zboží je nové (tzn. nepoužité, ani repasované),

3.7.3. zboží má vlastnosti, které si smluvní strany ujednaly a není-li takového ujednání, takové vlastnosti, které prodávající nebo výrobce popsal nebo které kupující očekával s ohledem na povahu zboží,

3.7.4. zboží se hodí k účelu, který vyplývá zejm. z této smlouvy,

3.7.5. zboží vyhovuje požadavkům právních předpisů,

3.7.6. zboží je bez jakýchkoli jiných vad, a to i právních.

4. Lhůta, místo a způsob plnění

4.1. Prodávající je povinen odevzdat předmět koupě do 6 týdnů ode dne účinnosti této Smlouvy.

4.2. Místem odevzdání zboží je Ostravská univerzita, Centrum informačních technologií, Bráfova 5, 702 00 Ostrava.

4.3. Osobou oprávněnou za prodávajícího je Jaroslava Bělinová, belinova@compunet.cz, tel.: 257 211 846 nebo 734 257 324.

4.4. Technický kontakt a zároveň osobou odpovědnou za převzetí předmětu plnění je Jiří Kubina, jiri.kubina@osu.cz, tel.: 553 46 1144 nebo 733 787 226.

4.5. Odevzdání zboží bude potvrzeno podpisem oprávněných osob prodávajícího a kupujícího na protokolu o odevzdání zboží s uvedením data odevzdání zboží.

4.6. Kupující po odevzdání zboží provede kontrolu zjevných vad. Zjistí-li kupující, že zboží má vady, oznámí to prodávajícímu nejpozději do 5 pracovních dnů ode dne odevzdání zboží. Má se za to, že dnem následujícím po uplynutí 5 pracovních dnů ode dne odevzdání zboží, aniž by kupující oznámil prodávajícímu existenci vad, kupující zboží převzal.

4.7. Kupující není povinen převzít zboží, které vykazuje vady, přestože by samy o sobě ani ve spojení s jinými nebránily řádnému užívání zboží nebo jeho

užívání podstatným způsobem neomezovaly. Nepřevezme-li kupující zboží z tohoto důvodu, hledí se na ně, jako by prodávajícím nebylo odevzdáno a prodávající je v prodlení oproti lhůtě dle čl. 4.1. Smlouvy se všemi důsledky, které jsou s tím spojeny.

4.8. Pokud věc vykazuje vady, popř. pokud prodávající neodevzdal kupujícímu některou z více kusů jedné položky zboží ve smluvené lhůtě, přičemž mělo být na základě této smlouvy odevzdáno více kusů jedné položky zboží, a kupující se přesto rozhodne odevzdané zboží od prodávajícího převzít, má se za to, že prodávající splnil závazek odevzdat věc s vadami. Prodávající v takovém případě není v prodlení s odevzdáním věci. Při oznamování a odstraňování vad věci dle tohoto článku postupují smluvní strany přiměřeně v souladu s ustanoveními o reklamaci vad věci uvedenými v čl. 8 této smlouvy. Takto oznámené vady se prodávající zavazuje odstranit v souladu s uplatněným právem kupujícího bezodkladně, nejpozději však do 10 dnů ode dne jejich oznámení prodávajícímu.

5. Cena a platební podmínky

5.1. Celková kupní cena za zboží dle čl. 3 této Smlouvy byla dohodou smluvních stran stanovena ve výši:

bez DPH	**1 073 700,- Kč**
DPH	**225 477,- Kč**
s DPH	**1 299 177,- Kč**

5.2. Sjednaná kupní cena je konečná a není možné ji překročit. Prodávající prohlašuje, že kupní cena obsahuje jeho veškeré nutné náklady spojené s řádným a včasným splněním závazků dle této Smlouvy, zejm. s řádným odevzdáním zboží kupujícímu.

5.3. Platba bude uskutečněna na základě daňového dokladu vystaveného Prodávajícím se splatností do 30 dnů ode dne doručení daňového dokladu Kupujícímu. Každý daňový doklad (faktura) bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Daňový doklad nesplňující předepsané náležitosti bude kupujícím vrácen do dne splatnosti daňového dokladu k opravě, lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nově vystaveného daňového dokladu. K faktuře bude přiložen dodací list s uvedením názvu a ceny zboží.

5.4. V jedné faktuře nesmí být současně fakturováno plnění hrazené z investičních i neinvestičních prostředků.

5.5. Prodávající je povinen zasílat faktury elektronickými prostředky na adresu financni.uctarna@osu.cz.

5.6. Povinnost kupujícího uhradit fakturu je splněna dnem připsání příslušné částky na účet prodávajícího.

5.7. Prodávající přebírá nebezpečí změny okolností ve smyslu § 1765 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“).

5.8. Kupující neposkytne prodávajícímu žádnou zálohu.

6. Smluvní pokuty

6.1. V případě prodlení prodávajícího s odevzdáním zboží kupujícímu oproti lhůtě stanovené v čl. 4.1 je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,3 % z ceny nedodaného zboží (včetně DPH) za každý i započatý den prodlení.

6.2. V případě prodlení prodávajícího s plněním povinností stanovených v čl. 8.12. této Smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 300,-- Kč za každý i započatý den prodlení.

6.3. V případě prodlení kupujícího s úhradou faktury proti sjednanému termínu je kupující povinen zaplatit prodávajícímu smluvní pokutu ve výši 0,3 % z dlužné částky za každý i započatý den prodlení.

6.4. Uplatněním nároku na smluvní pokutu není dotčeno oprávnění kupujícího požadovat náhradu škody způsobenou porušením povinnosti ze strany prodávajícího, které je zajištěno smluvní pokutou. To platí i tehdy, bude-li smluvní pokuta snížena rozhodnutím soudu.

7. Nebezpečí škody na zboží a přechod vlastnictví

7.1. Nebezpečí škody na zboží a vlastnické právo ke zboží přechází na kupujícího v okamžiku jeho převzetí kupujícím.

8. Záruka za jakost, Práva z vadného plnění

8.1. Zboží je vadné, neodpovídá-li této smlouvě.

8.2. Práva kupujícího z vadného plnění zakládá vada, kterou má zboží v době jeho odevzdání, v době mezi odevzdáním zboží a počátkem běhu záruční doby nebo v záruční době.

8.3. Smluvní strany sjednávají, že zboží bude odpovídat této smlouvě i po smluvenou záruční dobu.

8.4. Prodávající se zavazuje poskytnout na zboží záruku za jakost, přičemž záruční doba činí minimálně 24 kalendářních měsíců ode dne převzetí zboží, není-li u jednotlivých položek obsažených v Příloze č. 1 této Smlouvy, v záručním listu nebo v jiném prohlášení o záruce stanovena záruční doba delší. Prodávající má povinnosti z vadného plnění nejméně v takovém rozsahu, v jakém trvají povinnosti z vadného plnění výrobce zboží.

8.5. Záruční doba začíná běžet ode dne převzetí zboží kupujícím. Je-li zboží kupujícím převzato s alespoň jednou vadou, počíná záruční doba běžet až dnem odstranění poslední vady. Podobně bylo-li zboží kupujícím převzato i přes to, že prodávající neodevzdal některou z položek zboží ve smluvené lhůtě, počíná záruční doba běžet až dnem odevzdání chybějící položky zboží.

8.6. Záruční doba dle předchozího odstavce neběží po dobu, po kterou kupující nemůže zboží užívat pro vady, za které odpovídá prodávající, tedy i z důvodu jejich řešení.

8.7. Má-li zboží vadu (vady) má kupující právo:

8.7.1. na odstranění vady dodáním nového zboží bez vady,

8.7.2. na odstranění vady dodáním chybějícího zboží,

8.7.3. na odstranění vady opravou zboží (je-li vada opravou odstranitelná),

8.7.4. na přiměřenou slevu z kupní ceny, nebo

8.7.5. odstoupit od smlouvy.

Kupující je oprávněn si zvolit a uplatnit kterékoli z výše uvedených práv dle svého uvážení a s přihlédnutím k charakteru vady, příp. zvolit a uplatnit kombinaci těchto práv. Kupující sdělí prodávajícímu, jaké právo si zvolil zároveň s oznámením vady nebo bez zbytečného odkladu po oznámení vady.

8.8. Požadavek na odstranění vad kupující uplatní u prodávajícího nejpozději poslední den záruční doby, a to oznámením kontaktní osobě prodávajícího v písemné podobě nebo elektronicky na e-mail kontaktní osoby (dále také jen „reklamace“). I reklamace odeslaná kupujícím poslední den záruční doby se považuje za včas uplatněnou. V reklamaci kupující uvede alespoň popis vady a/nebo informaci o tom, jak se vada projevuje, a způsob, jakým požaduje vadu odstranit.

8.9. Prodávající se zavazuje prověřit reklamaci a do 3 pracovních dnů ode dne jejího doručení oznámit kupujícímu, zda reklamaci uznává. Pokud tak prodávající v uvedené lhůtě neučiní, má se za to, že reklamaci uznává a že vadu odstraní v souladu s touto smlouvou.

8.10. I v případech, kdy prodávající reklamaci neuzná, je povinen vadu odstranit. V takovém případě prodávající kupujícího písemně upozorní, že se vzhledem k neuznání reklamace bude domáhat úhrady nákladů na odstranění vady od kupujícího.

8.11. Pokud prodávající reklamaci neuzná, může být její oprávněnost ověřena znaleckým posudkem, který obstará kupující. V případě, že reklamace bude tímto znaleckým posudkem označena jako oprávněná, ponese prodávající i náklady na vyhotovení znaleckého posudku. Právo kupujícího na bezplatné odstranění vady i v tomto případě vzniká dnem doručení reklamace prodávajícímu. Prokáže-li se, že kupující reklamoval neoprávněně, je povinen uhradit prodávajícímu prokazatelně a účelně vynaložené náklady na odstranění vady.

8.12. 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.

8.13. 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.:

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

8.13.2. 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.

8.14. V případě, že prodávající neodstraní vadu ve lhůtě dle čl. 8.12. Smlouvy, nebo pokud prodávající odmítne vadu odstranit, je kupující oprávněn vadu odstranit na své náklady a prodávající je povinen kupujícímu uhradit náklady vynaložené na odstranění vady, a to do 10 dnů ode dne jejich písemného uplatnění u prodávajícího. V případech, kdy ze záručních podmínek vyplývá, že záruční opravy může provádět pouze autorizovaná osoba nebo kdy neautorizovaný zásah je spojen se ztrátou práv ze záruky, smí kupující vadu odstranit pouze využitím služeb autorizované osoby.

8.15. 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.

8.16. 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.

9. Ostatní ujednání

9.1. Kupující je povinným subjektem dle zákona č. 340/2015 Sb., o registru smluv (dále jen "zákon o registru smluv"). Prodávající bere na vědomí a výslovně souhlasí s tím, že tato smlouva včetně všech jejích změn a dodatků podléhá uveřejnění v Registru smluv (informační systém veřejné správy, jehož správcem je Ministerstvo vnitra). Kupující se zavazuje, že provede uveřejnění této smlouvy dle příslušného zákona o registru smluv.

9.2. V souladu s ustanovením § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, Kupující uveřejní na svém profilu zadavatele smlouvu včetně všech jejích změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.

9.3. Kupující zveřejní smlouvu včetně všech jejich změn a dodatků dle odstavce 9.1. a 9.2. tohoto článku v plném znění. V případě, že smlouva nebo dodatek obsahuje utajované informace, obchodní tajemství dle § 504 obč. zákoníku, osobní/citlivé údaje, práva duševního vlastnictví či jiné informace, které nelze poskytnout při postupu podle předpisů upravujících svobodný přístup k informacím (dále jen „chráněné informace"), je Prodávající povinen nejpozději v den uzavření smlouvy tuto skutečnost sdělit Kupujícímu, tyto informace přesně identifikovat a kvalifikovat právní důvod jejich ochrany. Tyto části smlouvy (chráněné informace) pak Kupujícím nebudou uveřejněny. V opačném případě je Prodávající seznámen se skutečností, že zveřejnění smlouvy v plném znění dle citovaných zákonů se nepovažuje za porušení obchodního tajemství a že smlouva neobsahuje ani jiné chráněné informace a Prodávající s jejím zveřejněním výslovně souhlasí.

9.4. Tato smlouva nabývá platnosti dnem jejího uzavření a účinnosti nejdříve dnem uveřejnění smlouvy v Registru smluv. O této skutečnosti Kupující Prodávajícího uvědomí.

9.5. Prodávající je dle ustanovení § 2 písm. e) a § 13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon

o finanční kontrole), v platném znění, osobou povinnou spolupůsobit při výkonu finanční kontroly.

9.6. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty). Tyto doklady budou uchovávány způsobem stanoveným platnými právními předpisy. Subjekty oprávněné k výkonu kontroly mají právo přístupu i k těm částem nabídek, smluv a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. jako obchodní tajemství, utajované skutečnosti) za předpokladu, že budou splněny požadavky kladené právními předpisy (např. zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), v platném znění). Oprávnění kontroly dle předchozí věty se vztahuje i na případné subdodavatele prodávajícího.

9.7. Ve věcech touto Smlouvou výslovně neupravených se bude tento smluvní vztah řídit ustanoveními obecně závazných právních předpisů, zejména občanským zákoníkem a předpisy souvisejícími.

9.8. Smlouva je vyhotovena ve dvou stejnopisech s platností originálu a každá ze smluvních stran obdrží po jejich podpisu jedno vyhotovení, pokud není smlouva uzavřena elektronicky.

9.9. Tato Smlouva může být měněna nebo doplňována pouze písemnými číslovanými dodatky podepsanými oprávněnými zástupci obou smluvních stran.

9.10. Kupující je oprávněn odstoupit od Smlouvy anebo jen částečně odstoupit od Smlouvy především v případě, že nebude uvolněna platba poskytovatele finančních prostředků (např. MŠMT) kupujícímu, nebo kupující nebude disponovat dostatečnými finančními prostředky, nebo že výdaje, které by kupujícímu na základě smlouvy měly vzniknout, budou kontrolním subjektem, označeny za nezpůsobilé. V takovém případě prodávající nebude uplatňovat nárok na náhradu škody a případné prodlení s placením daňových dokladů z tohoto důvodu.

9.11. Prodávající se zavazuje, že na fakturu uvede vždy takové bankovní spojení, které bude do tuzemské banky, a které bude mít v době vystavení a splatnosti faktury zveřejněno finančním úřadem na internetu, tak, jak to vyžaduje zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“), aby se kupující nedostal do pozice ručitele za odvod DPH za prodávajícího z důvodu platby na nezveřejněný či na zahraniční bankovní účet.

9.12. Pokud se prodávající do data splatnosti faktury stane tzv. nespolehlivým plátcem DPH ve smyslu ustanoven § 106a zákona o DPH a kupující se tak dostane do pozice, kdy dle zákona o DPH ručí za odvod DPH ze strany prodávajícího, je prodávající povinen o této skutečnosti kupujícího bezodkladně informovat.

9.13. Pokud se kupující dostane do pozice, kdy ze zákona ručí za odvod DPH za prodávajícího (např. z důvodů popsaných v bodě 9.11. nebo 9.12. tohoto článku), je kupující oprávněn uhradit prodávajícímu hodnotu faktury pouze ve výši bez DPH a DPH odvést na účet místně příslušného finančního úřadu

prodávajícího a prodávající s tímto postupem souhlasí. Dále v případě, že nastanou skutečnosti uvedené v bodě 9.11. tohoto článku, má kupující také právo pozastavit platbu celé částky závazku, a to do doby, než mu prodávající sdělí číslo takového bankovního účtu, který je veden v české bance a je zveřejněn finančním úřadem. Závazek se tím v obou případech považuje za splněný řádně a včas a kupující se nedostává do prodlení s úhradou. Prodávající pro tento případ prohlašuje, že jeho místně příslušným finančním úřadem pro DPH je Finanční úřad pro Prahu 5 a že v případě změny místně příslušného finančního úřadu bude kupujícího o této skutečnosti neprodleně informovat, jinak prodávající ponese případné náklady plynoucí ze skutečnosti, že částka DPH nebyla včas poukázána správnému finančnímu úřadu.

9.14. Ustanovení 19.11. až 19.13. se týkají Zhotovitele, kterému je přiděleno české DIČ.

9.15. Prodávající je povinen kupujícímu uhradit veškerou škodu, která mu vznikne nedodržením povinností uvedených výše v tomto článku, a navíc je kupující oprávněn odstoupit od této smlouvy. Odstoupení se stává účinným dnem jeho doručení prodávajícímu.

9.16. Smluvní strany po přečtení smlouvy potvrzují, že obsahu smlouvy porozuměly, že smlouva vyjadřuje jejich pravou, svobodnou a vážnou vůli, nebyla uzavřena v tísni či za nápadně nevýhodných podmínek a na důkaz této skutečnosti ji vlastnoručně podepisují.

Přílohy:
Příloha č. 1 – Technická specifikace předmětu plnění

Za Kupujícího dne …….

prof. MUDr. Jan Lata, CSc.
Digitálně podepsal prof. MUDr. Jan Lata, CSc.
Datum: 2019.12.05 13:32:15 +01'00'

prof. MUDr. Jan Lata, CSc.
rektor Ostravské univerzity

Za Prodávajícího dne 15.11.2019

Ing. Pavel Pikhart
Digitálně podepsal Ing. Pavel Pikhart
Datum: 2019.11.15 08:49:06 +01'00'

Ing. Pavel Pikhart
jednatel

Příloha č. 1 – Technická specifikace předmětu plnění

Zařízení pro uložení a analýzu logů

Dodávka a implementace systému pro centralizované ukládání a správu logů z libovolných zdrojů, s možností analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

Předmět:

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 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.

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 2.0". Platí však, že požadujeme, aby systém umožňoval on-line zobrazit data minimálně po dobu jednoho roku bez nutnosti obnovování dat ze záloh, případně modifikací v databázi systému. Uložená data musí být až do konce svojí retenční doby plně přístupná za všech okolností.

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.

Systém musí dále umožňovat bezztrátový sběr a příjem událostí ze zdrojů na pobočkách, a to vlastním řešením. Toto řešení zamezí ztrátě událostí během přenosu po mnohdy saturovaných 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.

Číslo	Popis - Řešení SEM/SIEM do 5000 událostí/sec. s minimálně 40TB velikostí databáze	Nabídnutá specifikace (účastník přesně popíše, jak nabízené zařízení plní požadovaný parametr)
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	
0	**Účastník uvede celý název a typ systému**	**LOGmanager-L**
1	Systém pracuje jako appliance s jedním uceleným 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.	Datasheet: https://www.logmanager.cz/#dokumenty
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz seznam podporovaných zařízení v Tabulka č. 1 – seznam zdrojů logů (pod touto specifikací))	viz Tabulka č. 1 – seznam zdrojů logů
3	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 bez vlivu na jeho ostatní funkce. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/toc.html#parsery
4	Parsery a alerty/korelace musí umožňovat použití matematických operací a nativní dekódování URL v těle zpráv.	ANO
5	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět klasifikaci vstupních dat pro rozhodovací procesy o jejich zpracování. Nepřipouští se nastavování klasifikace vstupních dat v čistě textovém formátu ani prostřednictvím editace makra nebo scriptu v rámci okna webového rozhraní. Předložte příslušný odkaz na dokumentaci popisující klasifikaci vstupních dat.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/parser/classifiers.html
6	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožňovat příjem logů i na uživatelsky definovaných UDP a TCP portech. Přijaté logy	Komunikační matice: https://doc.logmanager.cz/manual/3.2.4/cs/communication-matrix.html Nastavení ODBC Konektoru: https://doc.logmanager.cz/manual/3.2.4/cs/devices/sql-agents.html

	systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.	
7	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí.	ANO
8	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO
9	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO
10	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
11	Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Nepřipouští se konfigurace prostřednictvím vnořených skriptů nebo maker. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/parser/classifiers.html
12	Systém provádí konsolidaci logů na centrálním místě.	ANO
13	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.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/logs/reports.html
14	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
15	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. (Všechna data uložená v databázi systému jsou trvale dostupná a je možné je prohledávat v libovolném časovém období bez omezení či nutnosti manuálního otevírání či zpětného uzavírání datových polí databáze)	ANO
16	Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.	ANO
17	Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám.	ANO

18	V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.	ANO
19	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.	ANO
20	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 Viz potvrzení o shodě
21	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem systému nevratně modifikovat.	ANO
22	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
23	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO
24	Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.	ANO
25	Konfigurační a Systémové rozhraní a dokumentace 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 jednotivých vlastností navrhovaného systému.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/index.html
26	Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO
27	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.	ANO
28	Požadujeme, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO
29	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ANO
30	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.	Naleznete na uživatelském fóru: https://forum.logmanager.cz/

31	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)“.	Viz prohlášení výrobce o shodě
32	Jednotná centrální webová konzole 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 pro jednotlivé části systému s rozdílným ovládáním. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/index.html
33	Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí.	Systémové skupiny: https://doc.logmanager.cz/manual/3.2.4/cs/web/users/sysgroups.html Databázové skupiny: https://doc.logmanager.cz/manual/3.2.4/cs/web/users/dbgroups.html
34	Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes WMI protokol neumožňuje monitorovat textové logy.	ANO
35	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu.	ANO
	Minimální HW parametry požadovaného systému nebo subsystému pro virtualizované řešení	
36	Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	ANO
37	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.	ANO
38	2 procesory, min. 10 jader každý, s podporou HyperThreadingu.	ANO
39	Min. 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	ANO
40	Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 4GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	ANO
41	Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků	ANO

	určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	
42	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.	ANO
43	Větráky v systému musí být vyměnitelné za provozu a redundantní.	ANO
44	2x napájecí zdroje s redundancí napájení 1+1.	ANO
45	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	ANO
46	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ANO
	Výkonnostní a SW parametry systému	
47	Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli - viz bod 32, není nutné editovat žádné konfigurační soubory včetně IP adresace systému).	ANO
48	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli (viz bod 32). Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	ANO Release notes v českém jazyce: https://doc.logmanager.cz/manual/3.2.4/cs/release-notes.html
49	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.	Downgrade je možné spustit volbou verze software, a to během bootu zařízení z konzole appliance. LOGmanager zachovává poslední 4 verze operačního systému automaticky pro možný downgrade. Během downgrade nedojde k narušení konzistence uložených dat.
50	Průměrný trvalý příjem min. 5 tisíc událostí/s, s možností navýšení na minimálně 6 tis. událostí/s prostřednictvím licence nebo rozšíření hardware. Výkon musí odpovídat pro požadované množství událostí s průměrnou délkou 600Byte.	ANO
51	Špičkový příjem minimálně 10 tisíc událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí, než je průměrný trvalý příjem, je systém uloží do bufferu a zpracuje později.	ANO
52	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat.	ANO
53	Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz bod 32). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery 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.	ANO
54	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	ANO

55	Systém musí podporovat integraci externích informací.	ANO
56	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení. Pro snadnější editaci požadujeme vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládá testovací zpráva během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	ANO Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/parser/parsing_rule.html#pridani-parsovaciho-pravidla
57	V centrální správcovské konzoli (viz bod 32) je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.	ANO
58	V centrální správcovské konzoli (viz bod 32) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	ANO
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
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 nad databází. 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.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/system/cluster.html
61	Dvounodový cluster se chová jako 1 celek.	ANO
62	V případě využití dvou nodů v clusteru se zrychluje vyhledávání a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	ANO
63	V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu (řízenou aktivním prvkem počítačové sítě) a zároveň cluster musí zajišťovat synchronizaci událostí mezi nody.	ANO
64	Řešení musí obsahovat volitelnou podporu pro mezipaměť diskového subsystému na SSD nebo NVRAM typu o kapacitě minimálně 3TB.	ANO
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.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/system/backup.html#zaloha-obnova-konfigurace
66	Podpora zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování.	ANO

	Zálohy dat musejí být vhodně kompresovány. Zálohy musí systém umožnit obnovit a data ze záloh během obnovy znova indexovat tak, aby bylo možné v datech obnovených ze záloh pracovat shodně jako s aktuálním obsahem databáze. Zálohování musí jít kompletně nastavit v uživatelském rozhraní systému, nepřipouští se využívání scriptů, maker nebo textových konfiguračních souborů. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/system/backup.html
	Alerty	
67	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO
68	Text alertu musí být uživatelsky definovatelný s proměnnými z přijaté rozparsované události.	ANO
69	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO
70	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. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/logs/alerts.html
71	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém.	https://doc.logmanager.cz/manual/3.3.0/cs/web/logs/syslogOutput.html
72	V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha).	ANO
73	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.	ANO
	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. Předložte kompletní dokumentaci a poznámky k vydání (release notes) k agentu pro sběr událostí z prostředí Microsoft.	PDF s WES release notes je součástí partnerského toolkitu.
75	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	ANO
76	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole z bodu 32.	ANO
77	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. 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, zda 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.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/sources/windowsfilters.html#pridani-noveho-filtru
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 (viz bod 32). 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.	Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/web/sources/windows.html
79	Agent automaticky překládá zástupné kódy status ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	ANO
80	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	ANO
81	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ANO
82	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 32) 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.	Dokumentace Windows Agentů globálně: https://doc.logmanager.cz/manual/3.2.4/cs/web/sources/windowssettings.html Dokumentace nastavení vybraného Windows Agenta: https://doc.logmanager.cz/manual/3.2.4/cs/web/sources/windows.html#editace-klientske-stanice
83	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO
84	Počet instalací Windows agenta nesmí být licenčně omezen. *(případně požadujeme licenci na **2000** systémů.)*	ANO
	Podpora pro sběr událostí z poboček	
85	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 Dokumentace: https://doc.logmanager.cz/manual/3.2.4/cs/forwarder.html
86	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
87	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená	ANO

	data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	
88	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO
89	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO
90	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO
91	Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.	ANO
92	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO
93	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO
	Vysoká dostupnost, SW Podpora a záruka na hardware	
94	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.	ANO
95	HW - Požadovaná min. 4 letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	ANO
96	SW - Podpora výrobce na aktualizaci systému a parserů na minimálně **4 roky.** Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO
97	V rámci dodávky systému budou provedeny komplexní akceptační testy včetně simulací maximálního zatížení systému dle požadavků (viz bod 50 a 51)	ANO

2. Požadavky na školení:	**Nabídnutá specifikace (účastník přesně popíše, jak nabízenou službu splní)**
Součástí předmětu plnění bude komplexní školení na úroveň administrátor pro dodávaný systém centralizovaného ukládání a správy logů z libovolných zdrojů, s možností analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele. Školení bude pro 3 osoby v rozsahu min. 40 hodin a bude probíhat v sídle zadavatele /Bráfova 5 Ostrava/ na dodaném systému. Jako součást školení bude zahrnuta i možnost dodatečných konzultací v rozsahu 4 hodiny v sídle dodavatele.	ANO

Tabulka č. 1 – seznam zdrojů logů

Minimální seznam podporovaných zdrojů logů
Apache httpd
Apache Tomcat
Amavis
Antivir AVG
Antivir Avast
Antivir Eset
Antivir Eset Remote administrator
Brocade FC switches
ArcSight CEF format all sources
Barracuda Email Security Gateway
Cisco ASA
Cisco Firepower
Cisco IOS
Cisco IronPort
Cisco Nexus
Cisco SMB
Cisco WLC
Dell Force10
Dell iDrac (Server OoB management)
Dell PowerConnect
Dell SonicWALL
Dell W-series WiFi
Discard (Special distard rule)
Dropbear SSH (mostly Embedded Linux)
Extreme NAC
Extreme Networks XOS
FlowMon
FortiAuthenticator
FortiDDoS
Fortigate
FortiGate-Lite (performance optimized)
FortiMail
FortiManager
FreeRADIUS
Qradar LEEF format all sources
HAProxy (structured rfc5425 logformat)
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
CheckPoint via OPSEC protocol
ISC BIND

ISC DHCP
ISC DHCPD
JSON format all sources
Juniper SRX
Juniper SRX-Lite (performance optimized)
Kaspersky Endpoint Security
Kaspersky Security Center
Kerio Connect
Kerio Control
Kernun Clear Web
Kernun Web filter
Linux Cron
Linux Freeradius
Linux Iptables
Linux Postfix
Mikrotik
Microsoft Exchange log
Microsoft SharePoint
Microsoft SQL
Microsoft Windows DHCP log
Microsoft Windows DNS debug log
Microsoft Windows Firewall (optimized for performance)
Microsoft Windows IIS
MySQL
Nginx
Novell eDirectory
OpenSSH server
Oracle DB
Palo Alto Networks NGFW
PostgreSQL
Ruckuss wireless
Safetica DLP
SAP
Shorewall
SonicWall
Sophos
SpamAssasin
Squid (Web Proxy)
Squid for Windows
RFC5425 format all sources
Symantec Endpoint Protection Manager
Symantec Messaging Gateway (brightmail)
Synology NAS DSM
Trapeze
TrendMicro DeepDiscovery
TrendMicro TippingPoint NG-IPS
UBNT Rocket
UBNT UniFI
VMware
Windows - any logs from Event Viewer
Windows - any text log from file

Celková nabídková cena:

	Nabídková cena v Kč bez DPH	**DPH**	**Nabídková cena v Kč včetně DPH**
Řešení SEM/SIEM do 5000 událostí/sec. s minimálně 40TB velikostí databáze	983 700,-	206 577,-	1 190 277,-
Školení	90 000,-	18 900,-	108 900,-
Celková cena	1 073 700,-	225 477,-	1 299 177,-