SMLOUVA O DODÁVCE A IMPLEMENTACI SYSTÉMU PRO CENTRALIZOVANÉ UKLÁDÁNÍ A SPRÁVU LOGŮ Z LIBOVOLNÝCH ZDROJŮ

evid. č. ČIŽP: 9 - 20

Smluvní strany:

Česká republika - Česká inspekce životního prostředí
IČ: 416 93 205
se sídlem: Na Břehu 267/1a, Praha 9 – Vysočany, PSČ: 190 00
zastoupená: Ing. Erikem Geussem, Ph.D., ředitelem
(dále jen „objednatel“ nebo „ČIŽP“) na straně jedné

a

Caleum a.s.
IČ: 28351363
se sídlem: Na Pankráci 1724/129, Praha, PSČ: 140 00
zapsaná v obchodním rejstříku vedeném Městským soudem, oddíl B, vložka 18559
zastoupená:
bankovní spojení:
(dále jen „dodavatel“) na straně druhé

(objednatel a dodavatel dále též jen „smluvní strany“)

uzavřely níže uvedeného dne, měsíce a roku v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) a v souladu s příslušnými ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon o veřejných zakázkách“) tuto

smlouvu o dodávce a implementaci systému pro centralizované ukládání a správu logů z libovolných zdrojů:

Preambule

Smluvní strany uzavírají tuto smlouvu na základě výsledku zadávacího řízení na podlimitní veřejnou zakázku s názvem „Dodávka a implementace systému pro centralizované ukládání a správu logů z libovolných zdrojů“, zadávanou objednatelem jako zadavatelem ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon o veřejných zakázkách“) pod interním evidenčním číslem 09-20 (dále jen „veřejná zakázka“), v němž byla nabídka prodávajícího vybrána jako nejvhodnější.

Článek I.
Úvodní ustanovení

1. Účelem této smlouvy je vymezení práv a povinností smluvních stran při dodávce a implementaci systému pro centralizované ukládání a správu logů z libovolných zdrojů a všech souvisejících činnostech.

2. Pro plnění předmětu této smlouvy jsou závazné rovněž všechny dokumenty vztahující se k veřejné zakázce, a to výzva a zadávací dokumentace včetně, všech příloh vztahujících se k předmětu této smlouvy, a nabídka dodavatele.

3. Dodavatel výslovně prohlašuje, že se seznámil s výzvou a zadávací dokumentací veřejné zakázky, přičemž mu nejsou známy žádné nejasnosti či pochybnosti, které by znemožňovaly řádné plnění jeho závazků podle této smlouvy. Dodavatel se zavazuje, že plnění podle této smlouvy poskytne v souladu se zadávacími podmínkami veřejné zakázky a v souladu se svou nabídkou.

4. Dodavatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění této smlouvy, že mu jsou známy podmínky nezbytné pro její realizaci, a že disponuje takovými kapacitami a odbornými znalostmi, včetně technického a personálního zázemí, které jsou nezbytné pro realizaci této smlouvy za dohodnutou maximální smluvní cenu uvedenou ve smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

5. Dodavatel prohlašuje, že jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

Článek II.
Účel a předmět smlouvy

1. Dodavatel se touto smlouvou zavazuje:
   a) zhotovit návrh centrálního úložiště pro sběr a analýzu logů (dále jen "návrh centrálního úložiště“) umožňující:
      (i) dlouhodobé ukládání událostí, jejich analýzu a hlášením problémů (tzv. "Security Information Management" - dále jen "SIM"),
      (ii) monitoring infrastruktury, korelace událostí a alertování v reálném čase (tzv. "Security Event Management" - dále jen "SEM"); a
      (iii) následnou analýzu a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací;
   b) zhotovit centrální úložiště, včetně potřebného HW a SW (dále jen "centrální úložiště“);
   c) otestovat centrální úložiště v IT prostředí objednatele (dále jen „testování“);
   d) dodat a implementovat centrálního úložiště do IT prostředí objednatele; a
   e) dodat objednateli úplnou dokumentaci centrálního úložiště;
   f) poskytnout objednateli příslušné licence k centrálnímu úložišti a popř. souvisejících podlicencí v rozsahu stanoveném dále v této smlouvě;
   (dále jen „plnění“).

   Podrobná specifikace plnění je obsažena v příloze č. 1 této smlouvy. Rozsah akceptačních testů pro testování centrálního úložiště je obsažen v příloze č. 3 této smlouvy.

2. Objednatel se touto smlouvou zavazuje zaplatit dodavateli za řádně a včas poskytnuté plnění sjednanou cenu ve výši a za podmínek uvedených dále v této smlouvě.

3. Dodavatel prohlašuje, že je mu známo IT prostředí, ve kterém má centrální úložiště fungovat, včetně charakteru dat, která má zpracovávat.

Článek III.
Místa plnění a lhůta plnění

1. Místem plnění podle této smlouvy je sídlo ředitelství ČIŽP uvedené v záhlaví této smlouvy a sídla oblastních inspektorátů na níže uvedených adresách:
   - Oblastní inspektorát ČIZP Praha, Wolkerova 40/11, 160 00 Praha 6,

- Oblastní inspektorát ČIZP Brno, Lieberzeitova ul. 14, 614 00 Brno,
- Oblastní inspektorát ČIZP Ostrava, Valchařská 15, 702 00 Ostrava,
- Oblastní inspektorát ČIZP České Budějovice, U Výstaviště 16, 370 21 České Budějovice,
- Oblastní inspektorát ČIZP Plzeň, Klatovská tř. 48, 301 22 Plzeň,
- Oblastní inspektorát ČIZP Olomouc, Tovární 41, 772 00 Olomouc,
- Oblastní inspektorát ČIZP Ústí nad Labem, Výstupní 508/9, 400 07 Ústí nad Labem,
- Oblastní inspektorát ČIZP Liberec, Třída 1. máje 858/26, 460 01 Liberec,
- Oblastní inspektorát ČIZP Hradec Králové, Resslova 1229, 500 02 Hradec Králové,
- Oblastní inspektorát ČIZP Havlíčkův Brod, Bělohradská 3304, 580 01 Havlíčkův Brod,
- Oblastní inspektorát ČIZP Brno, pobočka ČIŽP ve Zlíně, třída Tomáše Bati 3792, 760 01 Zlín,
- Oblastní inspektorát ČIZP Ústí nad Labem, pobočka ČIŽP v Karlových Varech, Závodní 152, 360 18 Karlovy Vary.

Místem plnění pro předání dokumentace plnění (zejména dokumentace centrálního úložiště, manuály atp.) je sídlo ředitelství ČIŽP uvedené v záhlaví této smlouvy.

2. Přípravné a programovací práce je dodavatel oprávněn realizovat na svém vlastním technickém vybavení. Podle charakteru prací může dodavatel plnění realizovat i vzdáleným přístupem.

3. Dodavatel se zavazuje poskytnout plnění v níže uvedených etapách:
   a) část plnění specifikovaného v čl. II odst. 1 písm. a) této smlouvy do *9*[1] (slovy: *devíti*[1]) kalendářních dní od uzavření této smlouvy;
   b) část plnění specifikovaného v čl. II odst. 1 písm. b) a c) této smlouvy do *19*[1] (slovy: *devatenácti*[1]) kalendářních dní od uzavření této smlouvy;
   c) část plnění specifikovaného v čl. II odst. 1 písm. d) a e) této smlouvy do *24*[1] (slovy: *dvacetičtyř*[1]) kalendářních dní od uzavření této smlouvy.

4. Splněním předmětu smlouvy dodavatelem je poskytnutí celého plnění objednateli bez vad, právních vad a nedodělků. Tato skutečnost bude oběma smluvními stranami potvrzena podpisem protokolu o předání a převzetí plnění podle článku V. této smlouvy (dále jen akceptační protokol“).

Článek IV.
Cena plnění a platební podmínky

1. Celková cena plnění byla dohodou smluvních stran stanovena na 1 557 200,- Kč[1] Kč (slovy: *jedenmilionpětsetpadesátsedmtisícdvěstě* korun českých) bez DPH, přičemž cena plnění specifikovaného v:
   a) čl. II. odst. 1 písm. a) této smlouvy činí *126 000* Kč (slovy: *stodvacetšesttisíc* korun českých) bez DPH;
   b) čl. II. odst. 1 písm. b), c), d), e) a f) této smlouvy činí *1 431 200*[1] Kč (slovy: *jedenmiliončtyřistatřicetjednatisícdvěstě*[1] korun českých) bez DPH.

   K ceně plnění bude připočtena DPH v sazbě podle platných právních předpisů ke dni uskutečnění zdanitelného plnění. Sjednaná cena může být překročena pouze v souvislosti se změnou daňových předpisů týkajících se DPH, a to nejvýše o částku odpovídající příslušné legislativní změně, pokud se tato změna přímo vztahuje k předmětu smlouvy a nejedná se o obecnou změnu sazby DPH.

2. Sjednaná cena plnění je stanovena na základě nabídky dodavatele jako cena nejvýše přípustná a zahrnuje veškeré náklady dodavatele spojené s úplným provedením a předáním plnění, jakož i ceny za služby a dodávky, které nejsou výslovně uvedeny v zadávací dokumentaci veřejné zakázky nebo v této smlouvě, ale dodavatel jako odborník o nich ví anebo má vědět, že jsou nezbytné pro řádné splnění smlouvy. Dodavatel přebírá nebezpečí změny okolností ve smyslu ust. § 2620 odst. 2 občanského zákoníku.

3. Cena plnění bude objednateli vyúčtována po předání a převzetí plnění bez vad a nedodělků, tj. po jeho akceptaci bez výhrad podle článku V. odst. 2 písm. a) této smlouvy.

4. Daňový doklad – faktura dodavatele vystavená na základě této smlouvy musí mít náležitosti daňového dokladu stanovené zejména v ust. § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a v zákoně č. 563/1991 Sb., o účetnictví, v platném znění. Kromě těchto podstatných náležitostí musí faktura dodavatele obsahovat evidenční číslo smlouvy objednatele, číslo účtu dodavatele a všechny údaje uvedené v ust. § 435 odst. 1 občanského zákoníku, fakturovaná částka musí být vyjádřena výlučně v korunách českých.

5. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit dodavateli fakturu, která neobsahuje požadované náležitosti, která obsahuje cenu vyúčtovanou v rozporu se smlouvou nebo chybně vyúčtovanou DPH. Lhůta splatnosti vyúčtované ceny začíná v takovém případě znovu běžet ode dne doručení opravené faktury objednateli způsobem uvedeným v následujícím odstavci tohoto článku smlouvy.

6. Lhůta splatnosti cen vyúčtovaných fakturami dodavatele činí 21 (slovy: dvacet jedna) kalendářních dnů ode dne jejich doručení objednateli do datové schránky nebo doporučenou listovní zásilkou na adresu sídla ČIŽP uvedené v záhlaví této smlouvy nebo osobně do podatelny v sídle objednatele s výjimkou faktur vystavených v období od 1. do 31. 12., přičemž v tomto období je lhůta splatnosti cen plnění 60 (slovy: šedesát) dnů. Není-li ve smlouvě uvedeno jinak, platí stejná lhůta splatnosti i pro placení jiných plateb podle této smlouvy (smluvní pokuty, úroky z prodlení, náhrada škody apod.).

7. Cena plnění vyúčtovaná fakturou dodavatele se pokládá za uhrazenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch účtu dodavatele.

Článek V.
Akceptace plnění

1. Plnění poskytnuté podle této smlouvy se považuje za poskytnuté a akceptované objednatelem potvrzením akceptačního protokolu (dále jen „akceptační protokol“), podpisem osoby pověřené jednat za smluvní strany (článek XIII. této smlouvy). Smluvní strany se dohodly, že bude předána každá dílčí část plnění zhotovená v etapách podle harmonogramu uvedeného v článku III. odst. 3 této smlouvy.

2. Akceptační řízení je zahájeno dnem předložení akceptačního protokolu s výkazem práce a veškerých dalších případně potřebných podkladů objednateli, výsledkem akceptačního řízení mohou být tyto 3 stavy:
   a) Akceptováno bez výhrad: neshledá-li objednatel v poskytovaném plnění, resp. jeho dílčí části, žádné vady ani nedodělky, uvede do akceptačního protokolu, že plnění, resp. jeho dílčí část, akceptuje bez výhrad a akceptační protokol svými podpisy potvrdí oprávnění zástupci obou smluvních stran.
   b) Akceptováno s výhradami: v případě, že objednatel shledá v poskytovaném plnění, resp. jeho dílčí části, odstranitelné vady anebo nedodělky, které nebrání užití plnění, tj. nevyskytne-li se ve zhotoveném plnění, resp. jeho dílčí části, vedle vad kategorie B podle odstavce 3. tohoto článku smlouvy žádná vada kategorie A podle odstavce 4. tohoto článku smlouvy, stanoví objednatel po konzultaci s dodavatelem závazný přiměřený termín jejich odstranění. Objednatel do akceptačního protokolu uvede, že zhotovené plnění, resp. jeho dílčí část, akceptuje s výhradami, seznam vad a jejich kategorizaci do kategorií definovaných v odstavci 4. tohoto článku smlouvy. Oprávnění zástupci obou smluvních stran potvrdí akceptační protokol svými podpisy. Po odstranění všech vad provedou smluvní strany nové akceptační řízení za stejných podmínek.
   c) Neakceptováno: shledá-li objednatel v poskytovaném plnění, resp. jeho dílčí části, takové závažné vady anebo nedodělky, které brání jeho užití, tj. vyskytne-li se ve zhotoveném díle vedle vad kategorie B jedna nebo více vad kategorie A podle odstavce 4. tohoto článku smlouvy, stanoví po konzultaci s dodavatelem závazný přiměřený termín jejich odstranění. Objednatel do akceptačního protokolu uvede, že zhotovené

plnění, resp. jeho dílčí část, nebylo akceptováno a uvede seznam vad a jejich kategorizaci do kategorií definovaných v odstavci 4. tohoto článku smlouvy. Oprávnění zástupci obou smluvních stran potvrdí akceptační protokol svými podpisy. Po odstranění všech vad provedou smluvní strany nové akceptační řízení za stejných podmínek.

3. Předávací protokol potvrzující převzetí předmětu plnění (dále jen „předávací protokol“) objednatelem musí obsahovat alespoň tyto náležitosti:
   a) označení smluvních stran;
   b) datum a místo uzavření;
   c) obchodní název HW, výrobní číslo HW a identifikace SW užitých při zhotovení centrálního úložiště;
   d) počet a specifikace všech součástí, příslušenství a doplňků;
   e) seznam předávané dokumentace v českém jazyce v tištěné a elektronické podobě;
   f) prohlášení o shodě s označením CE;
   g) poznámku, že se předmět plnění přebírá bez výhrad, případně výhrady kupujícího k předmětu plnění a termín pro jejich odstranění;
   h) podpisy oprávněných zástupců smluvních stran, tj. pověřených osob uvedených v článku XIII. této smlouvy.

4. Pro účely ujednání odstavce 2 tohoto článku se sjednávají následující kategorie vad poskytovaného plnění, resp. jeho dílčí části:
   a) Vady kategorie A: kritické vady anebo nedodělky poskytnutého plnění, které ohrožují anebo mohou ohrozit řádné užití plnění, zejména: takový technologický postup, který na dané množině dat není buďto vůbec spustitelný, nebo spustitelný je, ale výsledek není v přiměřeném čase dosažitelný. Další kritickou vadou se rozumí takový návrh modelu, který nerespektuje technologické možnosti informačního prostředí ČIŽP. Kritickou vadou je i nedodržení běžných vlastností očekávaných od konsolidovaných dat, jako je např. zabezpečení datové integrity apod.;
   b) Vady kategorie B: ostatní vady anebo nedodělky poskytnutého plnění, které nespadají do kategorie A, tj. chyby neohrožující řádné užití plnění, např. nejasně zdokumentované postupy (např. nejednoznačná metadata či nekvalitní průvodní dokumentace).

5. Pro vyloučení všech pochybností smluvní strany sjednávají, že nedohodnou-li se objednatel s dodavatelem jinak, za přiměřený termín pro odstranění vad se pokládá:
   a) jeden týden u vad kategorie A;
   b) tři týdny u vad kategorie B.

Článek VI.
Další práva a povinnosti smluvních stran

1. Dodavatel se zavazuje:
   a) plnění podle této smlouvy poskytnout objednateli řádně a včas, v souladu s podmínkami této smlouvy a s platnými právními předpisy, podle svých nejlepších znalostí a schopností a s potřebnou odbornou péčí;
   b) na žádost objednatele spolupracovat a poskytnout potřebnou součinnost případným dalším smluvním partnerům objednatele anebo jiným osobám v souvislosti s realizací této smlouvy anebo jiných smluvních vztahů objednatele, pokud tato realizace souvisí nebo může souviset s poskytnutím plnění podle této smlouvy;
   c) předávat objednateli provozní, technickou, uživatelskou, administrátorskou a programátorskou dokumentaci vytvořenou anebo aktualizovanou při poskytování plnění podle této smlouvy jako podklad pro akceptační řízení;

d) i bez pokynů objednatele provést neodkladné úkony související s předmětem této smlouvy, které jsou nezbytné pro zamezení vzniku škody, anebo které lze s ohledem na předmět plnění veřejné zakázky a na znalosti dodavatele považovat za součást plnění veřejné zakázky. V případě takových úkonů bude smluvními stranami projednána a provedena případná úhrada ve smyslu ust. § 2908 občanského zákoníku;
e) zajistit, aby všechny osoby, které se na jeho straně podílí na plnění předmětu smlouvy, a které budou přítomny v prostorách ČIŽP, dodržovaly všechny bezpečnostní a provozní předpisy;
f) udržovat v platnosti a účinnosti po celou dobu trvání této smlouvy pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění ve výši minimálně 10.000.000 Kč (slovy: deset miliónů korun českých) na jednu škodní událost; na vyžádání je Dodavatel povinen tuto pojistnou smlouvu objednateli doložit kdykoli v průběhu trvání této smlouvy.

2. Objednatel se zavazuje:
a) poskytovat po celou dobu trvání této smlouvy dodavateli veškerou nezbytnou součinnost potřebnou k naplnění účelu smlouvy, zejména mu zajistit přístup do prostor místa plnění v rozsahu nezbytném pro poskytnuté plnění dle této smlouvy;
b) převzít od dodavatele bez zbytečného odkladu plnění, resp. jeho dílčí části, ve smyslu této smlouvy.

Článek VII.
Záruky

1. Dodavatel tímto poskytuje objednateli záruku za kvalitu poskytnutého plnění v délce 2 (slovy: dvou) let od jeho akceptace bez výhrad ve smyslu ujednání článku V. odst. 2 písm. a) této smlouvy.

2. Po celou dobu záruční doby je objednatel oprávněn požadovat bezplatné odstranění všech vad, které se na poskytnutém plnění vyskytnou a dodavatel je povinen takové vady bezplatně odstranit.

3. Objednatel je povinen vady plnění reklamovat u dodavatele bez zbytečného odkladu poté, co se o nich dozví, a to formou písemné reklamace, která musí vždy obsahovat alespoň číslo smlouvy, popis vady nebo informaci jak se vada projevuje. Reklamaci zašle objednatel dodavateli do datové schránky anebo doporučenou listovní zásilkou.

4. Dodavatel se zavazuje odstranit vady plnění, které se vyskytnou v průběhu záruční doby, vždy nejpozději do 3 (slovy: tří) dnů od doručení písemné reklamace, nedohodnou-li se smluvní strany jinak.

5. Neodstraní-li dodavatel vadu plnění reklamovanou v průběhu záruční doby v dohodnutém termínu, je objednatel oprávněn pověřit odstraněním vady jinou osobu. Dodavatel se v takovém případě zavazuje uhradit objednateli veškeré náklady vynaložené v souvislosti s odstraněním vady.

6. Záruční doba se prodlužuje o dobu, po kterou mělo plnění vadu bránící jeho řádnému užívání objednatelem, nebo po kterou bylo plnění mimo provoz z důvodu vady, na kterou se vztahuje záruka.

Článek VIII.
Vlastnické právo a licenční ujednání

1. V případě, že součástí předmětu plnění dodavatele na základě této smlouvy je zhotovení díla, jehož předmět se má stát vlastnictvím objednatele, přechází na objednatele vlastnické právo k takovému předmětu díla dnem uhrazení ceny za předmět plnění, resp. za jeho příslušnou část podle této smlouvy. Nebezpečí škody na takovém předmětu díla přechází na objednatele dnem jeho předání a převzetí objednatelem, resp. akceptací předmětu plnění objednatelem. Strany tímto výslovně sjednávají, že objednatel je oprávněn takové

dílo, resp. rozpracované dílo v přiměřeném rozsahu užívat pro testovací a zkušební provoz ještě před jeho předáním a před uhrazením ceny za poskytnutý předmět plnění. Stejně tak na objednatele přechází vlastnické právo ke všem zdrojovým kódům, klíčům a obdobným výstupům vzniklým při realizaci předmětu plnění na základě této smlouvy, a to dnem uhrazení ceny za předmět plnění, resp. za jeho příslušnou část podle této smlouvy (na základě které zdrojový kód, klíč nebo obdobný výstup vznikl). Strany tímto výslovně sjednávají, že objednatel je oprávněn zdrojový kód, klíč nebo obdobný výstup v přiměřeném rozsahu užívat pro testovací a zkušební provoz ještě před předáním plnění, včetně výstupů, jehož součástí jsou i zdrojové kódy, a tedy před uhrazením ceny za předmět plnění, resp. za jeho příslušnou část.

2. V případě, že výsledkem činnosti dodavatele podle této smlouvy je dílo, které naplňuje znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, včetně počítačového programu (dále jen „autorské dílo“), poskytuje dodavatel objednateli ve smyslu ust. § 2371 občanského zákoníku licenci, tj. oprávnění k výkonu práva autorské dílo užít, a to v rozsahu pro jeho řádné užívání k naplnění účelu této smlouvy a po celou dobu trvání příslušných práv.

3. Licenci podle předchozího odstavce uděluje dodavatel objednateli jako nevýhradní, k veškerým známým způsobům užití takového autorského díla, zejména k účelu, ke kterému bylo autorské dílo dodavatelem vytvořeno, a to minimálně v rozsahu nezbytném pro řádné užívání autorského díla objednatelem. Licence je udělena jako neodvolatelná, neomezená množstevním rozsahem, neomezená způsobem nebo rozsahem užití a teritoriálně neomezená. Dále je licence udělena na dobu určitou, a to po dobu trvání majetkových práv autora k autorskému dílu. Objednatel není povinen licenci využít a je oprávněn poskytnout třetím osobám sublicenci. Objednatel je oprávněn zpřístupnit užívání autorského díla svým zaměstnancům, zástupcům, právním nástupcům a dodavatelům (včetně dodavatelů outsourcingu), a to pouze pro vnitřní použití při současném zachování veškerých autorských práv dodavatele.

4. Povinnost týkající se poskytnutí licence v rozsahu podle předchozího odstavce platí pro dodavatele i v případě zhotovení části autorského díla poddodavatelem nebo třetí osobou.

5. Obsahem poskytnuté licence podle odst. 3. tohoto článku smlouvy je zejména oprávnění objednatele (popř. objednatelem pověřené třetí osoby) autorské dílo nebo jeho části rozmnožovat, zveřejnit, upravovat, zpracovávat, překládat či měnit jeho název, spojit dílo s dílem jiným a zařadit je do díla souborného.

6. Licenční odměny za veškerá oprávnění poskytnutá objednateli podle tohoto článku smlouvy jsou zahrnuty v ceně předmětu plnění podle této smlouvy.

7. Dodavatel se zavazuje, že výsledkem předmětu plnění nebo jakékoli jeho části nebudou porušena práva třetích osob. V opačném případě nese dodavatel vedle odpovědnosti za vady plnění i odpovědnost za veškeré škody, které tím objednateli vzniknou. Dodavatel se tímto výslovně zavazuje, že neopatří/nepoužije v rámci realizace předmětu plnění podle této smlouvy bez výslovného předchozího písemného souhlasu objednatele žádnou licenci od třetí osoby v souvislosti s předmětem plnění na základě této smlouvy, s níž by byl spojen vznik jakéhokoli závazku objednatele vůči dodavateli nebo třetí straně; v případě, že dodavatel tento svůj závazek poruší, nese veškeré náklady související s pořízením a užíváním takové licence.

8. V případě, že předmětem plnění dodavatele dle této smlouvy bude poskytnutí licencí k jakémukoli standardnímu SW třetích stran (včetně systémového SW, databází, a jiného SW, který nebyl vytvořen výlučně pro objednatele za účelem realizace této smlouvy), poskytne dodavatel objednateli k takovému plnění nevýhradní licenci v rozsahu nezbytném pro naplnění účelu této smlouvy, a to za podmínek stanovených v odst. 7 tohoto článku.

9. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací této smlouvy je dodavatel povinen vždy smluvně zajistit možnost nakládání s těmito právy objednatelem v rozsahu definovaném tímto článkem smlouvy.

Článek IX.
Ochrana osobních údajů, mlčenlivost

I. Ochrana osobních údajů:

1. Smluvní strany se zavazují zajistit povinnost mlčenlivosti všech svých pracovníků či jiných osob, jež budou přicházet do styku s osobními údaji, a to v tomto rozsahu:
   a) zachovávat mlčenlivosti o poskytnutých osobních údajích i o způsobu jejich zabezpečení;
   b) nezneužít osobní údaje ve prospěch svůj ani třetích osob;
   c) nevystavit osobní údaje přístupu neoprávněných osob ani nebezpečí jejich ztráty;
   d) zajistit povinnosti mlčenlivosti ohledně osobních údajů i po skončení plnění podle této smlouvy.

2. Smluvní strany berou na vědomí, že:
   a) každá ze smluvních stran je správcem osobních údajů (dále také jen „správce“) získaných od pracovníků smluvních stran v souvislosti s uzavřením této smlouvy (např. osobní údaje kontaktních osob);
   b) subjektem údajů se pro účely této smlouvy rozumí pracovník ČIŽP a pracovník dodavatele, jehož osobní údaje si smluvní strany poskytují v souvislosti s uzavřením této smlouvy;
   c) osobní údaje získané v souvislosti s uzavřením této smlouvy budou zpracovány v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR) a souvisejícími právními předpisy, výhradně za účelem realizace závazků z této smlouvy;
   d) osobní údaje získané v souvislosti s uzavřením této smlouvy nebudou poskytovány třetím osobám (příjemcem osobních údajů jsou výlučně smluvní strany navzájem a nebudou předávány třetím osobám ani příjemci ve třetí zemi);
   e) tato smlouva zároveň smlouvou o zpracování osobních údajů ve smyslu ust. § 34 zákona č. 110/2019 Sb., o zpracování osobních údajů s tím, že dodavatel má pro účely ochrany osobních údajů postavení zpracovatele a dále je povinen dodržovat ujednání obsažená v tomto ustanovení smlouvy;
   f) osobní údaje získané v souvislosti s uzavřením této smlouvy budou správcem uloženy po dobu nezbytně nutnou pro realizaci závazků z této smlouvy a pro splnění povinností správce plynoucích v souvislosti s uzavřením této smlouvy z platných právních předpisů.

3. Smluvní strany prohlašují a nesou odpovědnost za to, že jejich pracovníci stanovení smluvními stranami jako pověřené osoby podle článku XIII. této smlouvy byli poučeni:
   a) o tom, že smluvní strany si vzájemně předávají jejich osobní údaje v rozsahu: titul, příp. vědecká hodnost, jméno, příjmení, adresa elektronické pošty a telefonní číslo, v rámci plnění této smlouvy, a to za účelem realizace závazků z této smlouvy;
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči druhé smluvní straně, zejména právo na přístup k osobním údajům, které jsou o nich zpracovávány, právo na jejich opravu nebo výmaz nebo omezení zpracování, vznést námitku proti zpracování, jakož i uplatňovat další práva v mezích GDPR a právo podat stížnost k Úřadu pro ochranu osobních údajů.

II. Mlčenlivost:

4. Dodavatel se zavazuje zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním smlouvy dozvěděl nebo které objednatel označil za důvěrné, (dále jen „důvěrné informace"). Dodavatel nesdělí či nezpřístupní žádnou z důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování důvěrnosti informací se nevztahuje na informace, které se

staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících ze smlouvy, nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu.

5. Za důvěrné se nepovažují takové informace, které je objednatel, jako organizační složka státu, povinen zveřejňovat.

Článek X.
Sankce

1. V případě porušení závazků dodavatele při poskytnutí plnění podle této smlouvy je objednatel oprávněn požadovat po dodavateli zaplacení smluvní pokuty:

   a) ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý den prodlení se zhotovením a předáním jednotlivé dílčí části plnění objednateli oproti harmonogramu uvedenému v čl. III. odst. 3 písm. a) a b) této smlouvy;
   b) ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý den prodlení se zhotovením a předáním celého plnění objednateli oproti harmonogramu uvedenému v čl. III. odst. 3 písm. c) této smlouvy;
   c) ve výši 100.000 Kč (slovy: jedno stotisíc korun českých) do souhrnné maximální výše 500.000 Kč (slovy: pět set tisíc korun českých) za každý jednotlivý případ porušení závazku mlčenlivosti či ochrany důvěrných informací podle článku IX. této smlouvy anebo kteréhokoli závazku podle článku XII. této smlouvy;
   d) ve výši 2.000 Kč (slovy: dva tisíce korun českých) za každý jednotlivý případ porušení kterékoli jiné smluvní povinnosti, resp. za každý den prodlení se splněním takové povinnosti.

2. Smluvní pokuty jsou splatné dnem porušení příslušné smluvní povinnosti. Objednatel je oprávněn jednostranně započíst pohledávku z titulu smluvní pokuty proti jakékoli splatné pohledávce dodavatele za objednatelem. Dodavatel výslovně prohlašuje, že výše smluvních pokut sjednaná v předchozím odstavci je přiměřená a odpovídající charakteru zajišťovaných povinností.

3. Vedle smluvní pokuty je objednatel oprávněn požadovat po dodavateli zaplacení náhrady škody případně vzniklé porušením smluvní povinnosti dodavatele, a to v plné výši.

4. V případě prodlení objednatele s uhrazením ceny plnění je dodavatel oprávněn požadovat zaplacení úroků z prodlení ve výši podle platných právních předpisů k prvému dni prodlení.

Článek XI.
Odstoupení od smlouvy

1. Objednatel je oprávněn od této smlouvy odstoupit v případě podstatného porušení smluvních povinností dodavatelem s tím, že za podstatné porušení smluvních povinností se považuje zejména prodlení dodavatele s dodáním plnění nebo jeho části delší než 30 (slovy: třicet) kalendářních dnů po termínech dodání stanovených v článku III odst. 3. této smlouvy a porušení povinností stanovených v článku XII. odst. 1. této smlouvy.

2. Objednatel je dále oprávněn od této smlouvy odstoupit v případě, že zhotovitel neodstraní při akceptačním řízení podle čl. V. této smlouvy vady do 10 (slovy: deseti) dní u návrhu centrálního úložiště, 10 (slovy: deseti) dní u vad zjištěných při testování centrálního úložiště a 10 (slovy: deseti) dní u vad, které se vyskytnou při dodání a implementaci centrálního úložiště.

3. Zhotovitel je oprávněn od této smlouvy odstoupit v případě prodlení objednatele s úhradou ceny plnění delším než 14 (slovy: čtrnáct) kalendářních dnů.

4. Odstoupení od smlouvy se nedotýká práva na zaplacení smluvních pokut, úroku z prodlení, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany i po odstoupení od smlouvy.

5. V případě odstoupení od smlouvy nebo předčasného ukončení smlouvy na základě písemné dohody smluvních stran se smluvní strany zavazují poskytnout si vzájemně veškerou potřebnou součinnost k zamezení vzniku škody.

Článek **XII.**
Poddodavatelé

1. Dodavatel je oprávněn zajistit plnění svých závazků podle této smlouvy prostřednictvím poddodavatelů, jejichž specifikace včetně specifikace dílčích částí plnění, které budou těmito poddodavateli poskytovány, je obsažena v příloze č. 2 této smlouvy.

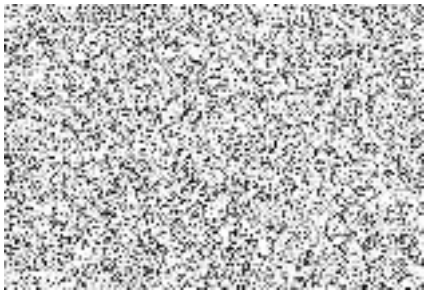
2. Dodavatel se zavazuje zajistit, že poddodavatelé budou jimi prováděné části plnění provádět v souladu se všemi podmínkami této smlouvy. Tím není dotčena výlučná odpovědnost dodavatele za poskytování řádného plnění podle této smlouvy. Dodavatel tedy odpovídá objednateli za řádné plnění části této smlouvy, které svěřil poddodavatelům, ve stejném rozsahu, jako by jej poskytoval sám.

3. Dodavatel je oprávněn změnit poddodavatele, prostřednictvím nichž zajišťuje plnění svých závazků podle této smlouvy, pouze z vážných objektivních důvodů a s předchozím písemným souhlasem objednatele. Objednatel se zavazuje souhlas se změnou poddodavatelů dodavateli bezdůvodně neodepřít.

Článek **XIII**
Osoby pověřené jednat za smluvní strany

Za účelem řádné realizace závazků podle této smlouvy jmenují smluvní strany tyto pověřené osoby ve věcech technických a administrativních:

Objednatel: 

Dodavatel: 

Článek **XIV.**
Vyšší moc

1. Jestliže některá ze smluvních stran není schopna dostát svým závazkům podle této smlouvy anebo je v prodlení v důsledku okolností, které nemůže ovlivnit ani předvídat v okamžiku jejich uzavření, nebude tato smluvní strana považována za smluvní stranu, která je v prodlení anebo která jiným způsobem porušila své

smluvní závazky a nebude po dobu trvání působení vyšší moci povinna k plnění těchto závazků, ani nebude povinna hradit smluvní sankce za porušení smluvní povinnosti.

2. Působení vyšší moci je dotčená smluvní strana povinna bez zbytečného odkladu po vzniku překážky vyšší moci písemně oznámit druhé smluvní straně.

3. V případě, že působení vyšší moci trvá déle než 60 (slovy: šedesát) kalendářních dní, je druhá smluvní strana oprávněna ukončit tuto smlouvu písemnou výpovědí s 30 (slovy třiceti) denní výpovědní lhůtou, která počne běžet prvého dne následujícího po doručení písemné výpovědi druhé smluvní straně.

Článek **XV.**
Závěrečná ustanovení

1. Tato smlouva a vzájemná práva a povinnosti z ní plynoucí se řídí právním řádem České republiky, zejména občanským zákoníkem, autorským zákonem a zákonem o zadávání veřejných zakázek.

2. Dodavatel souhlasí s tím, aby subjekty oprávněné podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, v platném znění, provedly finanční kontrolu závazkového vztahu vyplývajícího z této smlouvy s tím, že dodavatel se podrobí této kontrole a bude působit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona.

3. Dodavatel souhlasí s uveřejněním plného znění této smlouvy, s výjimkou neuveřejnitelných částí a údajů (z důvodů vyplývajících z platných právních předpisů), v souladu s povinnostmi objednatele podle platných právních předpisů, zejména podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění a podle zákona o registru smluv.

4. Dodavatel bere na vědomí, že je objednatelem veden v seznamu významných dodavatelů v souladu s vyhláškou o kybernetické bezpečnosti.

5. Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem jejího uveřejnění v registru smluv. Smluvní strany se dohodly, že uveřejnění této smlouvy v registru smluv podle zákona o registru smluv zajistí objednatel.

6. Neplatnost nebo neúčinnost některého ustanovení této smlouvy nezpůsobuje neplatnost celé smlouvy. Smluvní strany se zavazují nahradit neplatné nebo neúčinné ustanovení smlouvy ustanovením platným a účinným, které bude co do obsahu a významu neplatnému nebo neúčinnému ustanovení co nejblíže.

7. Veškerá oznámení podle této smlouvy musí být učiněna písemně a zaslána všem příslušným kontaktním osobám druhé smluvní strany prostřednictvím elektronické pošty, datové schránky nebo doporučenou poštou, případně předána osobně do podatelny Objednatele, není-li ve smlouvě výslovně uvedeno jinak.

8. Veškeré sporné záležitosti, které se vyskytnou a budou se týkat závazků vyplývajících z této smlouvy, budou smluvní strany prioritně řešit dohodou.

9. Jakékoli změny či doplnění této smlouvy je možné činit výhradně formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran.

10. Dodavatel je povinen bez zbytečného odkladu písemně oznámit objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky plnění této smlouvy, zejména změny svého majetkoprávního postavení, vstup do likvidace, úpadek, prohlášení konkursu, významné změny ovládání dodavatele podle

zákona č. 90/2012 Sb., o obchodních společnostech a družstvech, v platném znění (zákon o obchodních korporacích) nebo změny vlastnictví zásadních aktiv, popřípadě změny oprávnění nakládat s těmito aktivy, využívaných dodavatelem k plnění podle této smlouvy apod.

11. Jednacím jazykem mezi objednatelem a dodavatelem bude pro veškerá plnění vyplývající z této smlouvy a veřejné zakázky výhradně jazyk český, a to včetně veškeré dokumentace vztahující se k předmětu této smlouvy a zakázky, nedohodnou-li se smluvní strany u konkrétního dokumentu jinak (např. standardní technické specifikace výrobců HW v anglickém jazyce apod.).

12. Dodavatel není oprávněn postoupit ani převést jakákoli práva či povinnosti vyplývající z této smlouvy na třetí osobu bez předchozího písemného souhlasu objednatele.

13. Smluvní strany prohlašují, že si tuto smlouvu přečetly a s jejím obsahem souhlasí. Veškerá ujednání smluvních stran v jakékoli formě neobsažená v textu smlouvy jsou zcela nahrazena ujednáními této smlouvy.

14. Nedílnou součástí této smlouvy jsou tyto přílohy:
    Příloha č. 1: Technická specifikace plnění
    Příloha č. 2: Seznam poddodavatelů a částí jimi poskytovaného plnění
    Příloha č. 3: Technická specifikace minimálního rozsahu akceptačních testů při testování centrálního úložiště.

15. Tato smlouva byla vyhotovena ve třech vyhotoveních, z nichž dva stejnopisy obdrží objednatel a jeden stejnopis obdrží dodavatel.

V Praze dne …… 2020

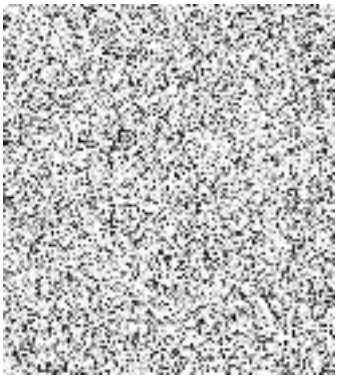
……

České inspekce životního prostředí

Ing. Erik Geuss, Ph.D.

ředitel

V Praze dne 23.8 2020



Technická specifikace, kontrolní seznam, akceptace

veřejné zakázky s názvem: „Dodávka a implementace systému pro centralizované ukládání a správu logů z libovolných zdrojů“

Technická specifikace - požadavky:

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 vhodným grafickým nástrojem s před-definovanými 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 bez účasti výrobce nebo dodavatele. Dokumentace musí poskytnout jednoznačný návod, jak takovéto parsery vytvářet, včetně 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.

Součástí dodávky musí být úplná dokumentace systému v češtině, obsahem i kvalitou srovnatelná s aktuální dokumentací v angličtině.

Technická specifikace – požadavky a kontrolní seznam:

Kontrolní seznam. Účastník povinně vyplní všechna pole vepsáním ANO nebo NE do tabulky kontrolního seznamu - sloupec „Splnění“. Nevyplnění položky sloupce „Splnění“ bude považované za nesplnění technické specifikace. Vyplnění sloupce „Hodnota/poznámka“ povinné není, účastník může doplnit údaj, upřesnění hodnoty nebo poznámku.

Číslo	**Popis - Řešení SEM/SIEM do 5000 událostí/s s minimálně 40TB velikostí databáze**	**Splňuje**	**Hodnota/ poznámka**
	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	1 HW aplikace spravovaná přes 1 rozhraní. Jako příloha nabídky je přiložen datasheet
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz tabulka podporovaných systémů uvedená níže)	Ano	LOGmanager splňuje veškeré systémy dle tabulky podporovaných systémů uvedených níže
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 není povinná konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se skripty/makra vkládají.	Ano	
4	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme	Ano	Dokumentace je na adrese viz: https://doc.logmanager.cz/manual/3.5.0/cs/web/toc.html#parsery

	předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.		
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	viz: https://doc.logmanager.cz/manual/3.5.0/cs/web/parser/classifiers.html
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. Předložte detailní komunikační matrici nabízeného systému a dokumentaci k nastavení ODBC v grafickém rozhraní systému.	Ano	Komunikační matice https://doc.logmanager.cz/manual/3.5.0/cs/communication-matrix.html ODBC: https://doc.logmanager.cz/manual/3.5.0/cs/devices/sql-agents.html
7	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	Ano	
8	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	Ano	

9	Standardizované pole dekódované z přijatých zpráv musí provádět minimálně tyto operace (pokud zdrojový log tyto informace obsahuje), názvy polí se můžou lišit, nicméně musí být v dodaném systému konzistentní - username = uživatelské jméno (malým písmem), src_ip = zdrojová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, dst_ip = cílová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, src_port = zdrojový port uložený v číselné podobě, dst_port = cílový port uložený v číselné podobě, protocol = druh přenosového protokolu, status = informace o stavu provedené akce (úspěch/neúspěch apod.), duration = kolik vteřin událost trvala uložena v číselné podobě.	Ano	
10	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	
11	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano	
12	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	Ano	
13	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	
14	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	Filtrování na úrovni klasifikace (nasměrovat provoz na parser Discard), v rámci parseru, v rámci alertu nebo na úrovni filtrů pro Windows zdroje. https://doc.logmanager.cz/manual/3.5.0/cs/web/parser/classifiers.html
15	Systém provádí konsolidaci logů na interním storage logovacího systému.	Ano	

16	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	https://doc.logmanager.cz/manual/3.5.0/cs/web/logs/reports.html
17	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	
18	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	
19	Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.	Ano	
20	Systém podporuje nativní získávání logů z Office365. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.	Ano	https://doc.logmanager.cz/manual/3.5.0/cs/web/sources/o365.html
21	V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.	Ano	Vyrovnávací paměť v nabízeném LOGmanageru není nižší než 50GB
22	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	Ano	
23	Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů.	Ano	Certifikát přiložen pod kontrolním seznamem

	Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.		
24	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	
25	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	
26	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano	
27	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	
28	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	https://doc.logmanager.cz/manual/3.5.0/cs/index.html
29	Systém nabízí kapacitní i výkonovou škálovatelnost.	Ano	
30	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.	Ano	Dostupná čistá kapacita je 40 TB
31	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	RAID v konfiguraci, kdy je možno vytáhnout dva disky
32	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	Ano	
33	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	Naleznete na uživatelském fóru: https://forum.logmanager.cz/ po registraci kapitola How to integrate LOGmanager with Zabbix či

			How to collect events from NAGIOS and parse them dále návod v pdf přidáváme jako součást nabídky
34	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	Certifikát přiložen pod kontrolním seznamem
35	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. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	Ano	Dokumentace je na adrese: https://doc.logmanager.cz/manual/3.5.0/cs/index.html
36	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	**Systémové skupiny:** https://doc.logmanager.cz/manual/3.5.0/cs/web/users/sysgroups.html **Databázové skupiny:** https://doc.logmanager.cz/manual/3.5.0/cs/web/users/dbgroups.html
37	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	
38	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	Ano	
	Minimální HW parametry požadovaného systému		

39	Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	Ano	2U včetně ližin
40	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	Ano	
41	2 procesory, min. 12 jader každý, s podporou HyperThreadingu.	Ano	
42	Min. 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	Ano	
43	Minimálně 40TB 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	Nabízené řešení má 40 TB čisté kapacity včetně SAS RAID řadiče s pamětí 8GB
44	Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	Ano	V nabízeném řešení je 12 ks stejných RAID disků
45	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad) ve webovém rozhraní systému a příslušný popis v dokumentaci.	Ano	
46	Větráky v systému musí být vyměnitelné za provozu a redundantní.	Ano	
47	2x napájecí zdroje s redundancí napájení 1+1.	Ano	
48	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	Ano	
49	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	Ano	V nabízeném řešení je Dell iDRAC
	Výkonnostní a SW parametry systému		
50	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli, například není nutné editovat žádné konfigurační soubory, scripty nebo makra).	Ano	
51	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	Ano	Release notes v českém jazyce: https://doc.logmanager.cz/manual/3.5.0/cs/release-notes.html Dále přikládáme v rámci nabídky

	poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.		
52	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	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.
53	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	V nabízeném řešení je zahrnut výkon na 5000 EPS s možno navýšení na 6000 EPS (pro průměrnou délku 600 Byte)
54	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	Špičkový výkon na 10 000 EPS/10 minut včetně podpory uložení do bufferu
55	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 40TB a nad to musí podporovat kompresi ukládaných dat.	Ano	Licenčně neomezený počet událostí v GB na den, čistá velikost databáze je 40 TB
56	Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. 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 a kontrolují syntaxi.	Ano	
57	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	Ano	
58	Systém musí podporovat doplňování zpráv o statické informace z textových tabulek. (Například k uživatelskému jménu doplnit informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové tabulky naplnitelné pomocí REST API	Ano	

	nabízeného systému a modifikovatelné přes webové rozhraní.		
59	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	Ano	https://doc.logmanager.cz/manual/3.5.0/cs/web/parser/parsing_rule.html#pridani-parsovaciho-pravidla
60	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	
61	V centrální správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	Ano	
62	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	
63	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	Ano	Dokumentace na https://doc.logmanager.cz/manual/3.5.0/cs/web/system/cluster.html

	obnovení po možném výpadku jednotlivých zúčastněných komponent.		
64	Dvounodový cluster se chová jako 1 celek. V případě využití dvou nodů v clusteru se zrychluje vyhledávání a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	Ano	
65	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 konfigurace a událostí mezi nody.	Ano	
66	Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.	Ano	Možnost rozšíření mezi paměti o SSD nebo NVRAM 3 je plně podporována
67	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	
68	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	Odkaz na dokumentaci: https://doc.logmanager.cz/manual/3.5.0/cs/web/system/backup.html#zaloha-obnova-konfigurace
69	Podpora zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Systém umožňuje obnovit data ze záloh a během obnovy je automaticky 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.	Ano	Zálohování dat je možno nastavit přímo v uživatelském rozhraní https://doc.logmanager.cz/manual/3.5.0/cs/web/system/backup.html
	Alerty		

70	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	Ano	
71	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	Ano	
72	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	Ano	
73	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	https://doc.logmanager.cz/manual/3.5.0/cs/web/logs/alerts.html
74	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	https://doc.logmanager.cz/manual/3.5.0/cs/web/logs/syslogOutput.html
75	V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality).	Ano	
76	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	
	Sběr událostí z Microsoft prostředí		
77	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.	Ano	Release notes jsou uvedeny jako příloha nabídky
78	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	Ano	

79	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.	Ano	
80	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	https://doc.logmanager.cz/manual/3.5.0/cs/web/sources/windowsfilters.html#pridani-noveho-filtru
81	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	https://doc.logmanager.cz/manual/3.5.0/cs/web/sources/windows.html
82	Agent automaticky překládá zástupné kódy status ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	Ano	
83	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	Ano	
84	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	Ano	
85	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	Dokumentace k Windows agentům https://doc.logmanager.cz/manual/3.5.0/cs/web/sources/windowssettings.html Dokumentace nastavení vybraného Windows Agenta: https://doc.logmanager.cz/manual/3.5.0/cs/

			web/sources/ windows.html#editace-klientske-stanice
86	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	Ano	
87	Počet instalací Windows agenta nesmí být licenčně a časově omezen.	Ano	zcela bez licenčního a časového omezení
	Podpora pro sběr událostí z poboček		
88	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	Rešeno v rámci LOGmanager forwarderu https://doc.logmanager.cz/ manual/3.5.0/cs/forwarder.html
89	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	
90	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	
91	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	Ano	
92	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	Ano	
93	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	Ano	
94	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	Ano	
95	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	Ano	
96	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	Ano	
	Vysoká dostupnost, SW Podpora a záruka na hardware		
97	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti	Ano	

98	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	
99	SW - Podpora výrobce na aktualizaci systému a parserů na **5 let.** Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	Ano	V řešení zahrnuta podpora na 5 let včetně aktualizace minimálně 4 x ročně

Tabulka podporovaných systémů

Minimální seznam podporovaných zdrojů logů
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 Firepower
Cisco ISE
Cisco IOS
Cisco IronPort
Cisco Nexus
Cisco SMB
Cisco UCS
Cisco WLC
CompuNet GAMA (on request)
Dell Force10
Dell iDrac (Server OoB management)
Dell Isilon
Dell PowerConnect
Dell SonicWALL
Dell W-series WiFi
Discard (Special distard rule)
Dropbear SSH (mostly Embedded Linux)
Epacs (http://www.epacs.cz/)
Extreme NAC
Extreme Networks XOS

FlowMon
FortiAuthenticator
FortiDDoS
Fortigate
FortiGate-Lite (performance optimized)
FortiMail
FortiManager
F5 BigIP ASM
FreeRADIUS
Greycortex NTA
Qradar LEEF (generický/standardizovaný formát)
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
JSON (generický/standardizovaný formát)
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
Lenovo XClarity (Server OoB management)
LOGmanager
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/webserver
Microsoft Windows IIS/ftpserver
MySQL
Nginx
Novell eDirectory
Office365
OpenSSH server
Oracle DB
Palo Alto Networks NGFW
PostgreSQL
Ruckuss wireless
Safetica DLP
SAP
Shorewall
SonicWall
Sophos
SpamAssasin
Stapro FONS Enterprise, Akord, Openlims
Squid (Web Proxy)
Squid for Windows
Radware Defense Pro
RFC5425 (generický/standardizovaný formát)
Symantec Endpoint Protection Manager
Symantec Messaging Gateway (brightmail)
Synology NAS DSM
Trapeze
TrendMicro DeepDiscovery
TrendMicro TippingPoint NG-IPS
UBNT Rocket
UBNT UniFI
VMware
Windows - any logs from Event Viewer
Windows - any text log from file

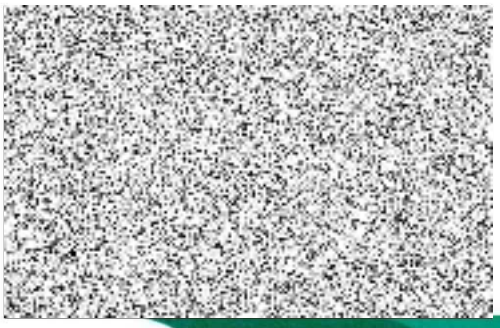
Certifikát o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů.

United Registrar of Systems Czech s.r.o.

PSN House
Argentinská 286/38
197 00 Praha 7
T: +420 266 314 892
F: +420 266 314 889
E: gen@urs-certifikace.cz
W: www.urs-certifikace.cz

Potvrzení o shodě produktu systém LOGmanager s normou ISO 27001:2013

Řešení „systém LOGmanager od společnosti Sirwisa a.s. IČ: 04667115 se sídlem Praha 5, Smíchov, Zubatého 295/5 splňuje požadavek normy ISO 27001:2013 na pořizování auditních záznamů.



United Registrar of Systems Czech s.r.o.

Argentinská 286/38
170 00 Praha 7
Česká republika

urs-czech.cz

videokurzy.online

Jsme tu pro Vás od roku 1994

United Registrar of Systems Czech s.r.o.

PSN House
Argentinská 286/38
197 00 Praha 7
T: +420 266 314 892
F: +420 266 314 889
E: gen@urs-certifikace.cz
W: www.urs-certifikace.cz

Potvrzení o zavedení systému ISO 27001:2013

Potvrzuji, že společnost Sirwisa a.s. IČ 04667115 má zavedeny a certifikovány požadavky Systému řízení bezpečnosti informací dle mezinárodního standardu ISO 27001:2013. Požadavky normy ISO 27001:2013 se vztahují na řešení systému LOGmanager od společnosti Sirwisa a.s., které zahrnuje pořizování a ukládání auditních záznamů.

Toto potvrzení se vydává na dobu platnosti příslušného akreditovaného certifikátu od naší společnosti č.: 74818/A/0001/UK/Cz platného do 18.7.2019

Společnost je vedena v obchodním rejstříku, vedeného Městským soudem v Praze oddíl C, vložka 78547. URS je členem United Registrar of Systems (Holdings) Limited.

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

Prohlášení o shodě

Výrobce: Sirwisa a.s., Zubatého 295/5, 150 00 Praha 5, IČ 046 67 115

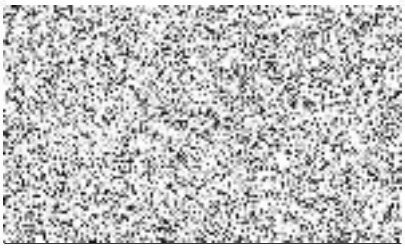
Výrobek: software LOGmanager

Určení: Nástroj pro centrální úložiště logů a SIEM (Security Information and Event Management) – management bezpečnostních informací a událostí.

Výrobce Sirwisa a. s. potvrzuje, že výrobek (respektive jeho software) je ve shodě s požadavky Vyhlášky 82 / 2018 Sb. v aktuálním znění ze dne 28. května 2018 „Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech 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)“ v aktuálním znění ze dne 7. března 2018.

Konkrétně výrobek / software splňuje požadavky §22 „Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů.“ a §24 „Sběr a vyhodnocování kybernetických bezpečnostních událostí.“. Dále poskytuje součinnost pro realizaci organizačních opatření dle §10 "Řízení provozu a komunikací", §12 "Řízení přístupu", §14 "Zvládání kybernetických bezpečnostních událostí a incidentů" a §16 "Audit kybernetické bezpečnosti".

V Praze dne 1. 8. 2019



Příloha č. 2: Seznam poddodavatelů a částí jimi poskytovaného plnění

Seznam poddodavatelů

Účastník:	
Název:	**Caleum a.s.**
Sídlo:	**Na Pankráci 1724/129, 140 00 Praha – Nusle**
IČO:	**28351363**

Pozn.:

podávající nabídku na podlimitní veřejnou zakázku s názvem:

Dodávka a implementace systému pro centralizované ukládání a správu logů z libovolných zdrojů

předkládá seznam poddodavatelů, kteří jsou mu známi:

Identifikační údaje poddodavatele	**Část plnění předmětu veřejné zakázky**

Pozn.: v případě, že účastník výběrového řízení nebude plnit veřejnou zakázku ani její žádnou část pomocí poddodavatelů, výše uvedenou tabulku **zřetelně přeškrtne**.

V Praze dne 13.8.2020

Podpis

(osoby oprávněné jednat jménem či za účastníka)

Příloha č. 3: Technická specifikace minimálního rozsahu akceptačních testů při testování centrálního úložiště.

Akceptace:

Podmínky akceptace - Ověření funkčních vlastností

Vybraný účastník obdrží od zadavatele výzvu k předložení funkčního testovacího vzorku, ten je povinen ho dodat na zadavatelem určenou adresu do doby dle smlouvy. Uchazeč poskytne vzorek včetně dokumentace bezplatně na období čtrnácti po sobě jdoucích dnů. Zadavatel v průběhu této lhůty provede na dodaném vzorku testování funkčních vlastností s použitím dodané dokumentace a 10. den předá zápis o průběhu a výsledku testování. Uchazeč v rámci testovacího provozu provede tyto práce:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním;
- Zapojení několika vybraných zdrojových systémů logů a událostí a otestování následujících vlastností:
    - nastavení klasifikace zdrojů,
    - nastavení značek (tagů),
    - filtrování událostí,
    - modifikace parsování existujícího zdroje v grafickém rozhraní nástroje;
- Konfigurace systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného systému
- Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému – viz Technická specifikace, všechny body z odstavce „Sběr událostí z Microsoft prostředí“
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele
- Otestování, jakým způsobem se v jednotném grafickém rozhraní vytvoří klasifikace a filtrování vstupních dat;
- Vytvoření, konfigurace a odladění jednoduchého uživatelsky definovaného parseru – viz Technická specifikace, odstavec „SW parametry“;
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz Technická specifikace, odstavec SW parametry
- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání zadavatele – viz Technická specifikace, odstavec SW parametry a odstavec Alerty (příklad 1: pošli alert jen v případě, že se událost stala na skupině Windows serverů X-krát během 10 minut; Příklad 2: pošli alert v případě, že uživatel za posledních 15 minut smazal na všech Windows serverech více než 30 souborů, bez započtení smazání dočasných souborů;)
- Odeslat událost, která vyvolala alert na externí syslog server přes TCP protokol
- Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
    - provedení zálohy konfigurace a dat na externí systém,
    - nastavení systému do továrního nastavení,
    - obnovení konfigurace a všech dat z vytvořených záloh,
    - kontrola úplnosti obnovené konfigurace a dat ze záloh;

- Navýšení a ponížení softwaru nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat. Kontrola změny funkčních vlastností po navýšení softwaru s ohledem na popis v poznámkách k danému vydání softwaru (release notes k jednotlivým testovaným verzím softwaru);
- Provést zálohování konfigurace a dat na externí systém, provést nastavení do továrního nastavení a obnovit konfiguraci a data alespoň jednoho pracovního dne ze zálohy
- Představení plnohodnotné dokumentace pro nabízený systém v českém jazyce
- Součástí ověření funkčních vlastností bude ověření požadované funkcionality a parametrů dodaného vzorku systému dle Technické specifikace tohoto zadání.

Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, dle dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to nejdéle do 3 pracovních dnů po doručení výzvy uchazeči. Testování bude probíhat v prostředí zadavatele. Po skončení testování bude funkční vzorek uchazeči vrácen (uchazeč si vyzvedne vzorek na vlastní náklady v místě plnění).

Testovací provoz bude zakončen akceptací a 10. den bude vyhotoven a předán Akceptační protokol. V případě, že testovaný systém neprojde úspěšným otestováním, může zadavatel vypovědět smlouvu a vyzvat k dodání testovacích vzorků účastníka, jehož nabídka se v hodnocení nabídek umístila jako další v pořadí.

Minimální rozsah akceptačních testů:

- Detailní parserování logů zařízení a systémů uvedených v požadavcích výběrového řízení
- Průměrný příjem min 5 tis událostí/s. Ověření v 10minutovém intervalu pomocí generátoru událostí.
- Špičkový příjem min 10 tis událostí/s, v případě vyššího počtu událostí je systém uloží do vyrovnávací paměti a zpracuje je později. Ověření v 10minutovém intervalu pomocí generátoru událostí.
- Konfigurace systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného systému
- Instalace Windows agenta na systémy požadované zadavatelem a jeho konfigurace
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz. Technická specifikace, odstavec SW parametry
- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání Zadavatele - viz. Technická specifikace, odstavec SW parametry a odstavec Alerty a odeslání události, která vyvolala alert na externí syslog server přes TCP protokol
- Součástí akceptačních testů bude ověření požadované funkcionality a parametrů dodaného systému dle Technické specifikace
- Uznání úplnosti dokumentace v českém jazyce ke všem komponentům dodaného systému

Sankce při nesplnění akceptačních testů:

Nebude-li dodané řešení do 30 dnů od dodání oboustranně akceptováno z důvodů zapříčiněných dodavatelem (tj. například že dodané řešení v akceptačních testech nesplní minimální požadované vlastnosti uvedené v Technické specifikaci), může být dodavatel sankcionován pokutou o výši 10% z nabízené ceny řešení.

Nebude-li dodané řešení do 60 dnů od dodání akceptováno z důvodů zapříčiněných dodavatelem (tj. například že dodané řešení v akceptačních testech nesplní minimální požadované vlastnosti uvedené v Technické specifikaci), může být sankce dodavateli navýšena na 15% z nabízené ceny řešení a důvodem k odstoupení od smlouvy.