[redacted]

SMLOUVA
O ZAJIŠTĚNÍ CENTRÁLNÍHO ÚLOŽIŠTĚ LOGU

Č. smlouvy Zadavatele: CES 2017/ 1047 **Č. smlouvy Poskytovatele: ANECT/PHA11/001**

Smluvní strany:

Městská část Praha 1
sídlo: Vodičkova 681/18, 115 68, Praha 1
IČ: 00063410
DIČ: CZ00063410
bankovní spojení: Česká spořitelna, pobočka Praha 1
číslo účtu: 27-2000727399/0800
jednající: Ing. Oldřichem Lomeckým, starostou městské části Praha 1

(dále jen „zadavatel")

a

ANECT a.s.
sídlo: Vídeňská 204/125, Přízřenice, 619 00 Brno
zapsaná ve veřejném rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 2113
IČ: 25313029
DIČ: CZ2531302
bankovní spojení: Komerční banka, a.s.
číslo účtu (CZK): 27-6667590237/0100
IBAN: CZ4001000000276667590237
zastoupená: Janem Zinkem, předsedou představenstva

(dále jen „poskytovatel")
(zadavatel a poskytovatel dále společně též jako „smluvní strany")

se níže uvedeného dne, měsíce a roku, v souladu s ustanoveními § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, s přihlédnutím k ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, dohodly na základě usnesení Rady MČ Praha 1 čUR17_1014 ze dne 11.9.2017 a vzájemného konsenzu o všech dále uvedených ustanoveních tak, jak stanoví tato:

I. Preambule

Tato smlouva je uzavírána na základě výsledků výběrového řízení zadávaného mimo režim zákona č. 134/2016 Sb. o zadávání veřejných zakázek, a to s odkazem na § 31 téhož zákona, pro zadání veřejné zakázky malého rozsahu s názvem „Centrální úložiště logů" (dále též „Veřejné zakázky") zahájené na základě výzvy k podání nabídek ze dne 21. 8. 2017.

Poskytovatel prohlašuje, že se náležitě seznámil se všemi zadávacími podmínkami veřejné zakázky malého rozsahu (dále jen „Zadávací dokumentace"), a které stanovují požadavky na předmět plnění Smlouvy, a že je odborně způsobilý ke splnění všech jeho závazků podle Smlouvy. Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou maximální smluvní cenu uvedenou ve Smlouvě. Poskytovatel prohlašuje, že nemůže nastat změna skutečností, které by plnění předmětu plnění dle této smlouvy podstatně ztěžovala.

Poskytovatel prohlašuje, že pokud by se v rámci plnění vznikla potřeba jiného úsilí nebo jiných nákladů, než bylo předpokládáno, nemá to vliv na cenu sjednanou v této smlouvě.
V případě jakékoliv nejistoty ohledně výkladu jednotlivých ustanovení Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel a cíle Veřejné zakázky vyjádřený a vyplývající ze Zadávací dokumentace a této Smlouvy.

II. Předmět smlouvy

Předmětem plnění dle této smlouvy ze strany poskytovatele je navrhnout, dodat a implementovat centrální úložiště logů pro sběr bezpečnostních událostí z kritických systémů, serverů a aplikací. Cílem je mít jednotné úložiště logů, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů.

Minimální požadavky a rozsah funkcionality plnění, které je poskytovatel povinen zajistit, jsou uvedeny v příloze č.1 této smlouvy (Technická specifikace). V příloze č. 2 je uvedena podrobná specifikace a popis dodávaného řešení.

Projekt bude realizován v následujících etapách:
1. etapa - Dodávka hardwaru a softwaru, implementace dodaného řešení do prostředí MČP1
2. – 5. etapa – Podpora dodaného řešení včetně servisu, dohledu a konzultací na příslušný rok

III. Cena plnění a způsob fakturace

Celková cena vzešlá z výsledků výběrového řízení u veřejné zakázky malého rozsahu představuje částku.

Celková cena bez DPH činí	**1.520.000,- Kč**
Zákonné DPH činí	**319.200,- Kč**
Celková cena včetně DPH činí	**1.839.200,- Kč**

Tato částka se stanovuje jako nejvýše přípustná a obsahuje veškeré náklady poskytovatele, včetně ostatních prací spojených s poskytováním plnění a nezbytné míry zisku.

Cena za jednotlivé části realizace je uvedená v následující tabulce:

Cena za dodané řešení (HW, SW) bez DPH	505.000,- Kč
Cena za instalaci a implementaci bez DPH	97.500,- Kč
Cena za podporu dodaného řešení na 1 rok bez DPH	85.000,- Kč
Cena za servis, dohled a konzultace dodaného řešení na 1 rok bez DPH	98.500,- Kč

Na základě zadavatelem odsouhlaseného a podepsaného Akceptačního protokolu je splatná cena za dodané řešení včetně ceny za instalaci a implementaci.

Cena za podporu dodaného řešení na první rok bude hrazena současně s fakturací za dodané řešení a instalaci. Podpora na další roky bude hrazena vždy ve výročí akceptace 1.etapy.

Cena za servis, dohled a odborné konzultace dodaného řešení na první rok bude hrazena současně s fakturací 1.etapy. Servis, dohled a odborné konzultace na další roky bude hrazen vždy ve výročí akceptace 1.etapy.

Oprávněně vystavený daňový doklad musí mít veškeré náležitosti daňového dokladu (faktury) dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Dále musí obsahovat i tyto údaje:

- pořadové číslo faktury, datum vystavení a datum splatnosti faktury, datum uskutečnění zdanitelného plnění;
- identifikaci poskytovatele podle Obchodního rejstříku, pakliže je v něm zapsán;
- označení banky a čísla účtu poskytovatele dle této smlouvy;
- celkovou fakturovanou částku bez DPH, vyčíslení sazby a výše DPH a celkovou cenu vč. DPH;
- evidenční údaje akce („název veřejné zakázky malého rozsahu“);
- vlastnoruční podpis vystavitele včetně kontaktního telefonního čísla;
- Akceptační protokol.

Délka splatnosti daňových dokladů (faktur) je 21 dnů od jejich doručení zadavateli.

V případě, že faktury nebude obsahovat potřebné náležitosti uvedené v předešlém odstavci, nebo bude obsahovat chybné či neúplné údaje (vč. chybně účtované ceny) či nebude připojen oboustranně podepsaný Akceptační protokol, je zadavatel oprávněn ji vrátit poskytovateli k opravě či doplnění s uvedením důvodu vrácení. Vrácení faktury musí být provedeno do data její splatnosti. Po vrácení faktury (nové či opravené) počíná běžet nová lhůta splatnosti.

Fakturovaná částka se považuje uhrazenou okamžikem jejího odepsání z účtu zadavatele.

IV. Doba plnění

Doba poskytování plnění zakázky dle smlouvy vzešlé z výběrového řízení je stanovena od září 2017 do 31. 10.2022.

Harmonogram plnění:

etapa	realizace
Etapa 1	Do 31.10.2017
Podpora, servis, dohled a odborné konzultace na 1. rok	akceptace 1.etapy + 1. rok (do 31.10.2018)
Etapa 2 – podpora na 2. rok	akceptace 1.etapy + 2 roky (do 31.10.2019)
Etapa 3 – podpora na 3. rok	akceptace 1.etapy + 3 roky (do 31.10.2020)
Etapa 4 - podpora na 4. rok	akceptace 1.etapy + 4 roky (do 31.10.2021)
Etapa 5 - podpora na 5. rok	akceptace 1.etapy + 5 roků (do 31.10.2022)

V. Způsob poskytování plnění, povinnosti smluvních stran

Poskytovatel se zavazuje, že bude při poskytování plnění postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy zadavatele. Poskytovatel se dále zavazuje dodržovat obecně závazné předpisy, technické normy a ustanovení této smlouvy.

VI. Místo plnění

Místem plnění poskytovatele je sídlo zadavatele a všechna jeho pracoviště v Praze. Smluvní strany mohou dojednat předávání výstupů plnění poskytovatele elektronickou cestou.

VII. Součinnost smluvních stran

Smluvní strany se zavazují poskytnout si vzájemně součinnost umožňující řádné plnění této smlouvy.
Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých závazků, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění smlouvy, jsou povinny o takové změně informovat druhou smluvní stranu nejpozději do tří pracovních dnů po provedení takové změny.
V zájmu optimálního plnění této smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze smluvních stran dostane do prodlení s plněním svých závazků, je povinna oznámit bez zbytečného odkladu druhé smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.
Smluvní strany se zavazují plnit své závazky v souladu se všemi příslušnými obecně závaznými legislativními předpisy.
Komunikace smluvních stran probíhá na úrovni oprávněných osob a jejich zástupců. Zástupci oprávněných osob přitom oprávněnou osobu zastupují v rámci její působnosti. Za tím účelem se stanovují následující osoby:

	Jméno a příjmení	Kontaktní telefon	Kontakt email
Zadavatel – oprávněná osoba	[redacted]		
Zadavatel - zástupce oprávněné osoby			
Poskytovatel – oprávněná osoba			
Poskytovatel – zástupce oprávněné osoby			

V případě doručování dokumentů v elektronické formě smluvní strany zavazují používat formát „.doc(x)“, nebo „.pdf“. Dokumenty v elektronické formě lze doručovat prostřednictvím elektronické pošty, prostřednictvím datové schránky nebo na dohodnutém datovém médiu.
Dokumenty se doručují na adresu poskytovatele uvedenou v záhlaví této smlouvy, není-li stanoveno nebo dohodnuto jinak.

VIII. Autorská a vlastnická práva:

Poskytovatel prohlašuje, že předmět Smlouvy ani jeho části, které jsou/mohou být autorským dílem poskytovatele, nemají žádné právní vady, že nejsou zatíženy právy třetích osob, a že poskytovatel je zcela oprávněn vykonávat veškerá majetková práva v celém rozsahu, s autorským dílem disponovat a uzavřít se zadavatelem smlouvu na celý rozsah předmětu plnění dle Smlouvy.

IX. Ochrana důvěrných informací:

Smluvní strany se zavazují zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním této Smlouvy dozvěděly, a to v rozsahu sjednaném v tomto článku Smlouvy. Za důvěrné informace jsou považovány jednak veškeré informace bez ohledu na formu jejich zachycení, které nebyly označeny jako veřejné a které se týkají Smlouvy, předmětu Smlouvy v ní sjednaného (zejména informace o právech a povinnostech smluvních stran, jakož i informace o cenách) či porušení zmíněné Smlouvy, dále (zejména, nikoliv však výlučně) obchodní tajemství, informace o činnosti příslušné smluvní strany, struktuře, hospodářských výsledcích, know-how), nebo případné informace, pro nakládání s nimiž je stanoven právními předpisy zvláštní režim utajení (osobní údaje, aj.), jednak informace, které byly jako důvěrné výslovně příslušnou smluvní stranou označeny; za důvěrné informace se však nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany jednou ze smluvních stran, dále informace získané na základě postupu nezávislého na této smlouvě, pokud je příslušná smluvní strana schopna tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany některé ze smluvních stran (dále jen jako „Důvěrné informace").

Poskytovatel je povinen Důvěrné informace ochránit proti úniku či neoprávněnému užití. Důvěrné informace mohou být Poskytovatelem využívány výlučně pro přípravu a poskytování předmětu smlouvy dle Smlouvy, není-li ve Smlouvě uvedeno jinak. Poskytovatel se zavazuje zachovávat mlčenlivost o Důvěrných informacích a zavazuje se, že přijme odpovídající opatření k ochraně Důvěrných informací.

Poskytovatel se zavazuje, že Důvěrné informace, které v souvislosti s poskytováním předmětu Smlouvy nebo při přípravě poskytování předmětu Smlouvy Poskytovateli poskytne Zadavatel, nebude bez písemného souhlasu Zadavatele žádným způsobem rozmnožovat (kromě potřebných kopií pro poskytnutí předmětu Smlouvy) a kdykoliv je na požádání vrátí Zadavateli, včetně všech případně vzniklých kopií a nosičů Důvěrných informací, nebo je na základě požadavku této smluvní strany zničí, včetně všech případně vzniklých kopií a nosičů Důvěrných informací.

Poskytovatel se zavazuje, že bez písemného souhlasu Zadavatele neposkytne Důvěrné informace v žádné formě třetím osobám. Poskytovatel je povinen zajistit, že jeho případný subdodavatel bude zachovávat mlčenlivost o Důvěrných informacích. Poruší-li subdodavatel Poskytovatele povinnost mlčenlivosti ve vztahu k Důvěrným informacím, považuje se to za porušení povinnosti mlčenlivosti Poskytovatele.

Za porušení povinnosti mlčenlivosti se nepovažuje, je-li Poskytovatel, jeho zaměstnanec, spolupracující osoba, zástupce nebo další osoba v obdobném postavení povinen Důvěrnou informaci sdělit na základě zákonem stanovené povinnosti.

Poskytovatel je povinen uvědomit Zadavatele o porušení povinnosti mlčenlivosti nebo ochrany Důvěrných informací podle Smlouvy bez zbytečného odkladu poté, co se o takovém porušení dozví.

Povinnost mlčenlivosti a ochrany Důvěrných informací podle Smlouvy trvá po dobu účinnosti Smlouvy a dále 3 (slovy: tři) roky po jejím ukončení.

Vzhledem k veřejnoprávnímu charakteru Zadavatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné ustanovení této Smlouvy nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě, včetně jejích příloh a případných dodatků Smlouvy za podmínek vyplývajících

z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

X. Odpovědnost za způsobenou škodu, záruka za jakost plnění, vady plnění:

Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a Smlouvy.
Poskytovatel odpovídá za škodu rovněž v případě, že část plnění poskytuje prostřednictvím třetí osoby – tzv. subdodavatele. Poskytovatel se zavazuje uhradit zadavateli či orgánu veřejné moci veškeré finanční částky, které budou poskytovateli ve správním, soudním či jiném obdobném řízení uloženy jako pokuty či jiné majetkoprávní sankce za poskytovatelem způsobené porušení právních povinností.
Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu Občanského zákoníku. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost a bránící řádnému plnění Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

XI. Zánik smlouvy

Tato smlouva primárně zaniká uplynutím předpokládané doby. Před uvedeným datem smluvní strany dále mohou ukončit smluvní vztah písemnou dohodou obou smluvních stran. Konečně, tato smlouva může zaniknout i jednostrannou výpovědí či odstoupením od smlouvy.

Zadavatel je oprávněn odstoupit od této smlouvy:
- v případě, že probíhá insolvenční řízení proti majetku poskytovatele, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek poskytovatele byl zcela nepostačující;
- v případě podstatného porušení této smlouvy poskytovatelem, zejména v případě kdy poskytovatel využil k plnění předmětu této smlouvy subdodavatele v rozporu s nabídkou poskytovatele v rámci výběrového řízení nebo bez předchozího souhlasu zadavatele,

Zadavatel je také oprávněn odstoupit od této smlouvy v případě, kdy vyjde najevo, že poskytovatel uvedl v rámci výběrového řízení nepravdivé či zkreslené informace, které by měly zřejmý vliv na výběr poskytovatele pro uzavření této smlouvy.

Smluvní strany jsou oprávněny od této smlouvy dále odstoupit za podmínek stanovených občanským zákoníkem nebo jinými právními předpisy.

Odstoupení od smlouvy musí být učiněno písemným oznámením o odstoupení od této smlouvy druhé straně, účinky odstoupení nastávají dnem doručení oznámení druhé straně. V pochybnostech se má za to, že odstoupení bylo doručeno do 10 dnů od jeho odeslání v poštovní zásilce s dodejkou, resp. do 10 dnů od jeho odeslání prostřednictvím informačního systému datových schránek.

Zadavatel je oprávněn smlouvu vypovědět písemnou výpovědí s 2 měsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet dnem doručení výpovědi poskytovateli.

XII. Rozhodné právo, řešení sporů.

Právní vztahy vyplývající z této smlouvy o dílo se řídí zákony České republiky, zejména zákonem č. 89/2012 Sb., občanským zákoníkem.
Smluvní strany se zavazují vyvinout maximální úsilí k smírnému odstranění a vyřešení sporů vzniklých z této smlouvy operativně, a to zejména prostřednictvím oprávněných osob nebo statutárních orgánů.
V případě, že spor nebude vyřešen konsensem podle předchozího odstavce, smluvní strany se dohodly řešit spor před soudem. Soudem příslušným pro všechny spory vzniklé z této smlouvy mezi zadavatelem a poskytovatelem je obecný soud zadavatele, v případě právního nástupce zadavatele nebo osoby, na níž byla převedena práva a povinnosti zadavatele ze smlouvy obecný soud této osoby.

XIII. Závěrečná ustanovení.

Tato Smlouva nabývá platnosti v den podpisu této Smlouvy a účinnosti dnem uveřejnění v registru smluv Ministerstva vnitra ČR, v souladu se zákonem č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), včetně důsledků porušení této povinnosti. Povinnost uveřejnit smlouvu v registru smluv MV ČR náleží městské části Praha 1.

Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v Centrální evidenci smluv (CES) vedené zadavatelem, která je veřejně přístupná a obsahuje údaje o smluvních stranách, předmětu Smlouvy, číselné označení této Smlouvy a datum jejího podpisu i v případné evidenci smluv zadavatele.

Veškeré změny či doplnění této Smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků Smlouvy.

Tato Smlouva je vyhotovena ve čtyřech vyhotoveních, z nichž zadavatel obdrží dvě vyhotovení a poskytovatel také dvě vyhotovení.

Seznam příloh:

Příloha č.1	Požadovaná technická specifikace
Příloha č.2	Podrobná specifikace a popis dodávaného řešení (vyplní dodavatel)

V Praze dne 27-09-2017 .....

[redacted]

V PRAZE dne 20-09-2017 .....

[redacted]

Příloha č.1 - Požadovaná technická specifikace

A. ÚVOD

Tato příloha popisuje základní specifikaci předmětu veřejné zakázky malého rozsahu, kterou je Dodávka a implementace centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů a aplikací zadavatele.
Požadujeme navrhnout, dodat a implementovat centrální úložiště logů pro sběr bezpečnostních událostí z kritických systémů, serverů a aplikací.
Nutností je možnost procházení těchto logů vhodným grafickým nástrojem s před-definovanými pravidly pro rychlé vyhledávání (například 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 a monitoring privilegovaných účtů, sdílených účtů a změn konfigurací apod.)
Cílem je mít jednotné úložiště logů, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nutnosti je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů.
Systém musí umožňovat tvorbu uživatelsky definovaných parserů bez účasti výrobce nebo dodavatele.

B. POŽADAVKY NA ROZSAH FUNKCIONALITY

Číslo	Popis	Splňuje
	Obecné parametry	
1	Zpracování událostí z různých zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	ano
2	Možnost dopsání parseru pro zařízení aktuálně nepodporované výrobcem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému.	ano
3	Systém standardizuje přijaté logy do jednotného formátu a logy jsou parserovány (rozdělovány) do příslušných políček dle jejich typu.	ano
4	Nad takto standardizovanými daty systém automaticky vytváří indexy pro rychlejší vyhledávání pro všechna pole standardizovaného logu.	ano
5	Všechny rozparsované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ano
6	Systém nesmí umožnit mazání nebo modifikování již uložených logů.	ano
7	Konsolidace logů na centrálním místě.	ano
8	Snadné vyhledávání událostí (ad hoc) bez nutnosti programování.	ano
9	Grafické znázornění událostí (grafy událostí).	ano
10	Grafické znázornění TOP událostí nad všemi daty za určité časové období.	ano
11	Automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě.	ano
12	Automatické doplňování reverzních DNS záznamů k IP adresám.	ano
13	V případě přetížení systému jsou události ukládány do vyrovnávací paměti.	ano
14	Unifikované vyhledávání napříč všemi typy dat a zařízení.	ano

15	Potvrzení, vystavené autorizovanou osobou, o shodě, že nabízený produkt splňuje požadavky normy ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo společnost výrobce nabízeného systému. Nelze nahradit čestným prohlášením.	ano
16	Možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	ano
17	Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů.	ano
18	Předpřipravené pohledy na uložená data.	ano
19	Aktualizace reportů a pohledů výrobcem.	ano
20	Konfigurační a Systémové rozhraní a On-line dokumentace v Českém jazyce.	ano
21	Kapacitní i výkonová škálovatelnost.	ano
22	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data musí být minimálně 40TB.	ano
23	Požadujeme, aby ze systému bylo možné vytáhnout 2 libovolné disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ano
24	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ano
25	Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 316 / 2014 ze dne 15. prosince 2014 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti“ ze dne 23. července 2014.	ano
26	Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému.	ano
27	Uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému.	ano
28	Možnost ověřovat uživatele systému na externím LDAP serveru.	ano
	HW parametry	
29	Jedna hardwarová appliance o velikosti max. 2U.	ano
30	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.	ano
31	HW 12Gb SAS RAID řadič s podporou RAIDu 0/1/5/6/10/50/60 s cache min. 2GB, která je zálohována baterií nebo flash pamětí.	ano
32	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.	ano

33	Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.	ano
34	2x napájecí zdroje s redundancí napájení 1+1.	ano
35	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ano
36	Požadovaná min. 5 letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	ano
	SW parametry	
37	Zařízení funguje formou appliance (všechny části systémů je možné nastavit v centrální webové správcovské konzoli - není nutné editovat žádné konfigurační soubory včetně IP adresace systému).	ano
38	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální webovou správcovskou konzoli.	ano
39	Průměrný příjem min. 6 tis událostí / s.	ano
40	Špičkový příjem 30 tis událostí / s, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později.	ano
41	Licenčně neomezený počet zařízení pro příjem zasílaných událostí.	ano
42	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 obrázků, které obsahují aplikační logiku.	ano
43	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	ano
44	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.	ano
45	V centrální webové správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.	ano
46	V centrální webové správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	ano
47	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
48	Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active / active.	ano
49	Vícenodový systém se chová jako 1 celek.	ano
50	V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	ano

51	Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru.	ano
52	V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody.	ano
	Alerty	
53	Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.	ano
54	Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události.	ano
55	Předpřipravené sety/vzory alertů výrobcem.	ano
56	Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	ano
57	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
	Sběr událostí z Microsoft prostředí	
58	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 souborových logů.	ano
59	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	ano
60	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální webové správcovské konzole.	ano
61	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální webové správcovské konzole. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	ano
62	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému . Správa a aktualizace Windows agenta se neprovádí z Group Policy.	ano
63	Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	ano
64	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	ano
65	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ano
66	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.	ano
67	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ano

68	Počet instalací Windows agenta nesmí být licenčně omezen. (případně požadujeme licenci na 700 systémů.)	ano, bez omezení
	Sběr událostí z poboček	
69	Systém musí umožňovat rozšíření o řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	ano
70	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
71	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ano
72	Řešení pro sběr dat z poboček musí mít výkon minimálně 2 tisíc událostí /s. a to i v trvalé zátěži.	ano
73	Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.	ano
74	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi.	ano
75	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ano

C. ROZSAH PODPORY (MAINTENANCE)

- standardní podpora řešení na dobu 60 měsíců – odstraňování chyb řešení, poskytování systémových, bezpečnostních a aplikačních update, držení hotline pro hlášení chyb v pracovní době (po-pá 9-17)
- záruka na dodané řešení na dobu 60 měsíců – uplatněná u autorizovaného partnera nebo v servisním středisku výrobce
- Podpora výrobce na aktualizaci systému a parserů na 60 měsíců.

D. ROZSAH SERVISU, DOHLEDU A KONZULTACÍ (ODBORNÉ PODPORY)

- Požadovaná doba 60 měsíců
- Servisní podpora slouží k odstranění vzniklých závad (HW/SW) v pracovních dnech v době 8:00 – 19:00 (5x11).
- Dohled je služba sloužící k monitorování, vyhodnocování, detekci a spolupráci při řešení mezních a poruchových stavů v rozsahu 24 hodin denně. Nahlášení Zadavateli do 30 minut.
- Odborná podpora v rozsahu 2 člověkohodin měsíčně, nevyčerpané hodiny se převádějí. Součástí je profylaxe, změny v nastavení pravidel, změny v konfiguraci, konzultace. Forma je telefonická, písemná nebo v místě Zadavatele.

Příloha č.2 - Podrobná specifikace a popis dodávaného řešení

Určení systému LOGmanager

LOGmanager je systém pro centralizovanou správu eventů a logů z libovolných zdrojů – operačních systémů a aplikačního software, síťových bezpečnostních zařízení a dalších. Je založen na novém typu databáze se škálovatelnou kapacitou a výkonným systémem prohledávání a prezentace nalezených dat. Jeho podstatou je sběr a ukládání všech relevantních eventů a logů organizace a jejich ukládání. Umožňuje prohledávat enormní množství dat v reálném čase. Výstupy prohledávaní jsou prezentovány v textové i grafické podobě s vysokou mírou interakce vzhledem k nalezeným datům. Systém umožňuje dlouhodobě ukládat data v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu a bezpečnostní audity.
LOGmanager není jen pro bezpečnostní nebo provozní oddělení IT. Velkým přínosem je i pro operační a provozní úseky, které mohou snadnou interakcí proti databázi událostí nalézt například podstatu nefunkčnosti systému, identifkovat možné závady a rychle dohledat události popisující příčinu konkrétního problému, ztráty dat nebo výpadku komunikace.
LOGmanager byl vyvinut jako systém pro centralizovanou správu protokolů událostí (logů) poskytující jednoduché zobrazení všech strojově generovaných dat v organizaci. V prvním kroku LOGmanager shromažďuje, sjednocuje a dlouhodobě uchovává protokoly událostí a záznamy o událostech z aktivních síťových prvků, bezpečnostních zařízení, operačních systémů a aplikačního softwaru. Následně v „téměř reálném čase" (near real-time) převádí shromážděná data do dobře definované výkonné databáze, ke které mohou IT bezpečnostní specialisté přistupovat prostřednictvím předdefinovaných řídicích panelů a strukturovaného i fulltextového vyhledávání s grafickým zobrazením výsledků. To může být použito, mimo jiné, i pro plnění účelu bezpečnostních opatření specifikovaných ZKB. LOGmanager navíc poskytuje i výkonné aplikační rozhraní podporující integraci s dalšími nástroji používanými v organizaci pro účely monitorování i zabezpečení.

Podporovaná zařízení

- Cisco, HP, Huawei, Fortinet, Juniper, Checkpoint a další
- Windows servery a stanice
- Linux servery
- Hlavní aplikace a databáze (SAP, MS-SQL, MySQL a další)
- VMware

Součástí systému je Windows Event Center – klient pro stanice a servery. Klient je centrálně spravovaný a umožňuje sběr logů z operačních systémů Windows. Tyto logy je možné filtrovat a kódované údaje v nich obsažené jsou překládány do srozumitelné formy

Klíčové vlastnosti

- Centrální úložiště logů pro Vaši organizaci
- Centrální přehled s grafickou prezentací – dashboards
- Rychlé vyhledávání
- Forenzní analýza
- Korelace událostí
- Alerting
- Reporting
- Sjednocení formátu logů
- Dlouhodobé uložení
- Plní požadavky Zákona o kybernetické bezpečnosti a ČSN ISO 27001 pro pořizování auditních záznamů
- Uchování logů pro předložení organizacím zabývajících se bezpečností CESNET CERT a CSIRT nebo Policii ČR
- Ukládání logů ze všech síťových a bezpečnostních zařízení, serverů, stanic
- Sběr logů pro řešení provozních problémů a bezpečnostních incidentů
- Intuitivní a rychlé vyhledávácí rozhraní
- Ověření přijetí záznamu do úložiště (pokud je podporováno odesílajícím zařízením)
- Ověření identity zdroje záznamů, aby nemohl být záznam podvržen (pokud je podporováno odesílajícím zařízením)

Konkurenční výhody

- Trvalý příjem až 5.000 událostí za sekundu
- Špičkový příjem až 10.000 událostí za sekundu
- Neomezený počet zdrojů
- V základu uložení až 30TB logů se snadným škálováním výkonu i úložné kapacity
- Interní diskové pole RAID 6 s ochranou proti výpadku disků
- Možnost zálohování na SMB/NFS systémy organizace
- Snadný a přehledný systém licencování bez skrytých nákladů
- Administrační rozhraní a dokumentace v českém jazyce
- Přímá technická podpora výrobcem