;itech

SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená dle ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, mezi:

I.
Smluvní strany

Objednatel: **Brněnské komunikace a.s.**
se sídlem, Renneská třída 787/1a, 639 00 Brno - Štýřice
IČO: 60733098
DIČ: CZ60733098
bankovní spojení: [redacted]
účet č. [redacted]
zapsán v OR u Krajského soudu v Brně, oddíl B, vložka 1479
zastoupen Ing. Luďkem Borovým, generálním ředitelem, na základě plné moci
ve věcech technických [redacted]
středisko 1800 - oddělení výpočetní techniky
číslo smlouvy objednatele: 1800 – 22000184

a

Poskytovatel: VISITECH, a.s.
se sídlem Košinova 655/59, 612 00 Brno, Královo Pole
IČO: 25543415
DIČ: CZ25543415
bankovní spojení: [redacted]
účet č.: [redacted]
zapsán dne v OR u Krajského soudu v Brně , oddíl B, vložka 6323
zastoupen
číslo smlouvy poskytovatele: SS/2004/2022

II.
Předmět smlouvy

(1) Předmětem této smlouvy je poskytování služeb spočívajících v zajištění provozu a bezpečnosti Log managementu infrastruktury pro následující části infrastruktury objednatele:

1. Sběr log dat z komponent datové komunikační infrastruktury,
2. Sběr log dat z bezpečnostních perimetrů,
3. Sběr dat z hardware komponent server a ze storage komponent (SNMP trap),
4. Sběr log dat z operačních systémů Microsoft Windows a Unix/Linux,
5. Sběr log dat z databázových strojů,
6. Sběr log dat z aplikačních strojů – WWW servery,

a to v souladu s podmínkami této smlouvy o poskytování služeb (dále také jen „smlouva") a se zadávacími podmínkami veřejné zakázky na tyto služby s názvem **„Logmanagement"**, v jejímž rámci je tato smlouva uzavírána (dále jen „služba").

(2) Podrobná specifikace poskytovaných služeb je vymezena v příloze č. 1 této smlouvy – Technická specifikace.

(3) Součástí poskytovaných služeb jsou dodávka a implementace systému nutného ke splnění předmětu plnění plynoucího z odst. 1 této smlouvy (dále „systém") a rovněž podpora provozu systému a poskytování operativních služeb po dobu 36 měsíců.

III.
Termín poskytnutí služeb a místo plnění

(1) Poskytování služeb bude zahájeno: dnem nabytí účinnosti této smlouvy, nejdříve však 1.5.2022
(2) Poskytování služeb bude ukončeno: 30.4.2025
(3) Místo plnění: Brno

IV.
Cena za poskytování služeb

(1) Cena za poskytování služeb v místě plnění a blíže upřesněných v příloze č. 1 byla dohodou smluvních stran stanovena takto:

	Cena bez DPH při dodávce	Cena bez DPH / měsíc	Cena bez DPH / 36 měsíců
Dodávka systému:	647 990,00 Kč	-	-
Služby podpory provozu:	-	34 000,00 Kč	1 224 000,00 Kč
Celkem:	-	-	1 871 990,00 Kč

(2) Uvedená cena je cenou nejvýše přípustnou, zahrnuje veškeré náklady a vedlejší výkony nutné k řádnému poskytování služeb a nelze ji zvýšit ani pod vlivem změny cen vstupů nebo jiných vnějších podmínek.
(3) Ke změně ceny může dojít pouze v případě dodatečných změn v rozsahu poskytovaných služeb odsouhlasených oběma smluvními stranami nebo pokud v průběhu poskytované služby dojde ke změně sazeb daně z přidané hodnoty.

V.
Platební podmínky

(1) Objednatel uhradí smluvní cenu postupně, placením skutečně a řádně provedených služeb v jednotlivých měsících, na základě soupisu skutečně provedených služeb potvrzeného oběma smluvními stranami.
(2) Faktura je daňovým dokladem a musí být vystavena v souladu s § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Poskytovatel se zavazuje dodat fakturu objednateli na email: [redacted] nebo na adresu společnosti Brněnské komunikace a.s., Renneská třída 787/1a, 639 00 Brno – Štýřice.
(3) Poskytovatel se zavazuje na daňovém dokladu pro platbu ceny služeb uvádět pouze bankovní účet, který určil správci daně ke zveřejnění v registru plátců a identifikovaných osob. Poskytovatel a objednatel se dohodli, že pokud bude na daňovém dokladu uveden jiný bankovní účet než ten, který je zveřejněn správcem daně v registru plátců a identifikovaných osob, objednatel je oprávněn provést úhradu daňového dokladu na tento účet zveřejněný podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a nebude tak v prodlení s úhradou ceny služeb. Pokud by objednateli vzniklo ručení v souvislosti s neplněním povinnosti poskytovatele vyplývajících ze zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, má objednatel nárok na náhradu všeho, co za poskytovatele v souvislosti s tímto ručením plnil.

(4) Objednatel je oprávněn vrátit fakturu poskytovateli až do data její splatnosti, jestliže obsahuje neúplné nebo nepravdivé údaje. Při nezaplacení takto nesprávně vystavené a doručené faktury není objednatel v prodlení se zaplacením. Poskytovatel je povinen fakturu řádně opravit a doručit ji objednateli s novou lhůtou splatnosti.
(5) Každá faktura je splatná do 30 dnů od jejího doručení objednateli.
(6) Poskytovatel je povinen uvádět na všech daňových dokladech (fakturách) číslo objednávky, číslo smlouvy objednatele a číselný kód Klasifikace produkce (CZ-CPA).
(7) Zálohové platby se nesjednávají.

VI.
Další povinnosti smluvních stran

(1) Poskytovatel je povinen dodržovat právní a technické podmínky vyplývající ze závazných platných právních předpisů, vyhlášek a norem.
(2) Poskytovatel je povinen zajistit autorskoprávní nezávadnost plnění. Pokud poskytovatel při plnění této smlouvy užije výsledek činnosti třetího subjektu chráněný právem průmyslového nebo jiného duševního vlastnictví, autorským právem apod., a uplatní-li oprávněná osoba z tohoto titulu své nároky vůči objednateli, poskytovatel provede na své náklady vypořádání majetkových důsledků a je odpovědný za jakoukoli újmu způsobenou objednateli.

VII.
Předání a převzetí služby

(1) Předání a převzetí bude sepsáno a potvrzeno předávacím protokolem vyhotoveným za součinnosti obou smluvních stran.
(2) U předávacího řízení je poskytovatel povinen doložit veškeré potřebné doklady. V případě dodávky systému jde zejména o:
- úplnou a podrobnou dokumentaci systému v českém jazyce,
- doklad o souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

VIII.
Odpovědnost za vady

(1) Poskytovatel odpovídá za odbornou úroveň poskytovaných služeb dle této smlouvy. Právo na náhradu újmy vzniklé neodborným provedením poskytovaných služeb se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
(2) Poskytovatel tímto čestně prohlašuje, že má oprávnění k činnosti v rozsahu této smlouvy a je účasten pojištění z odpovědnosti za újmu vzniklou jinému v souvislosti s poskytováním služeb.
(3) Poskytovatel poskytuje na provedení služeb záruku v délce **36 měsíců**, která začíná běžet ode dne předání každé jednotlivé služby. Poskytovatel je povinen odstranit vady každé jednotlivé služby, tj. odchylky od výsledku stanoveného touto dohodou, které se projeví v průběhu trvání záruční doby. Objednatel je povinen uplatňovat u poskytovatele práva z poskytnuté záruky písemně, nejpozději do 30 dnů po zjištění vad, na něž se záruka vztahuje. Poskytovatel je povinen vadu odstranit bezodkladně, nejpozději do jednoho měsíce od obdržení písemnosti, ve které je záruka uplatňována, nedohodnou-li se strany jinak.

IX.
Další ujednání

(1) Smluvní strany se zavazují, že bez předchozího písemného souhlasu druhé strany nevyzradí třetím osobám technické ani obchodní informace druhé strany, které se dozvěděly v souvislosti s plněním dle této smlouvy.

(2) Poskytovatel se zavazuje (v prostorách a na pracovištích objednatele) postupovat při plnění této smlouvy s odbornou péčí a zavazuje se dodržovat právní a technické předpisy a ostatní podmínky uložené mu smlouvou nebo veřejnoprávními orgány a dále zejména tato ustanovení:

- § 100 a násl. zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů,
- nařízení vlády č. 495/2001 Sb., kterým se stanoví rozsah a bližší podmínky poskytování osobních ochranných pracovních prostředků, mycích, čisticích a dezinfekčních prostředků, ve znění pozdějších předpisů,
- nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví zaměstnanců při práci, ve znění pozdějších předpisů, ve znění pozdějších předpisů,

tak, aby byla zajištěna bezpečnost pracovníků poskytovatele a třetích subjektů po celou dobu poskytování služeb.

(3) Poskytovatel je povinen upozornit objednatele ihned na nesprávnost jeho pokynů nebo podkladů, jinak odpovídá objednateli za újmu tím způsobenou.

(4) Poskytovatel je povinen plnit veškeré zákonné povinnosti v oblasti BOZP ve smyslu § 101 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, ve vazbě na zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci, ve znění pozdějších předpisů, zejména zakotvené v § 16 písm. b) tohoto zákona, a prováděcí nařízení vlády č. 591/2006 Sb., o bližších minimálních požadavcích na bezpečnost a ochranu zdraví při práci na staveništích, ve znění pozdějších předpisů. Poskytovatel je dále povinen zajistit zejména dodržování veškerých bezpečnostních, hygienických a ekologických opatření a opatření vedoucích k požární ochraně, a to v rozsahu a způsobem stanoveným příslušnými právními předpisy.

(5) Poskytovatel odpovídá za bezpečnost a ochranu zdraví při práci pracovníků realizující sjednané služby, přitom je povinen všechny tyto osoby vybavit ochrannými pracovními pomůckami. Dále je povinen provést u svých pracovníků vstupní školení o BOZP a o požární ochraně, jakož i zajistit, aby byla taková školení provedena i u svých subdodavatelů a jejich pracovníků. Tato školení je povinen průběžně obnovovat a kontrolovat u veškerých pracovníků znalosti o BOZP a o požární ochraně.

(6) Poskytovatel je povinen provádět vlastní dozor a soustavnou kontrolu nad dodržováním všech zásad BOZP a požární ochrany. Přitom je povinen dbát pokynů koordinátora BOZP objednatele a poskytnout mu veškerou zákonem upravenou součinnost k zajištění povinností v oblasti BOZP.

(7) Dojde-li v rámci plnění této dohody či při činnostech s ní souvisejících k jakémukoliv úrazu, je poskytovatel povinen zabezpečit jeho vyšetření a sepsání příslušného záznamu o takové události. Objednatel je povinen poskytnout za tímto účelem poskytovateli nezbytnou součinnost.

(8) Poskytovatel i objednatel jsou povinni se navzájem informovat o tom, že se dostali do úpadku ve smyslu § 3 zák. č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů.

(9) Poskytovatel prohlašuje, že neumožňuje výkon nelegální práce ve smyslu zák. č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a ani neodebírá žádné plnění od osoby, která by výkon nelegální práce umožňovala. V případě, že se toto prohlášení ukáže v budoucnu nepravdivým a vznikne ručení objednatele ve smyslu ust. zák. č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, má objednatel nárok na náhradu všeho, co za poskytovatele v souvislosti s tímto ručením plnil.

(10) Poskytovatel na sebe přebírá nebezpečí změny okolností dle ustanovení § 1765 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

X.
Sankce

(1) Jestliže se objednatel bezdůvodně opozdí s platbou ceny poskytovaných služeb, může vůči němu poskytovatel uplatňovat úrok z prodlení ve výši 0,2 % z dlužné částky za každý započatý den prodlení.
(2) V případě prodlení poskytovatele s poskytováním služeb nebo s jejich předáním bez zavinění objednatele může objednatel vůči poskytovateli uplatňovat smluvní pokutu ve výši 3.900,- Kč za každý jednotlivý případ prodlení a za každý započatý den prodlení.
(3) V případě nedostupnosti služeb spočívajících v poskytování podpory provozu systému nebo nedostupnosti služeb spočívajících v zajištění provozu rozhraní mezi objednatelem a poskytovatelem pro operativní služby delší než 12 hodin, může objednatel vůči poskytovateli uplatňovat smluvní pokutu ve výši 3.900,- Kč za každých 12 hodin prodlení.
(4) V případě, že poskytovatel poruší své povinnosti dle čl. IX., může vůči němu objednatel uplatňovat smluvní pokutu ve výši 10.000,- Kč za každé takové porušení.
(5) Při prodlení poskytovatele s odstraněním vady poskytovaných služeb může objednavatel vůči poskytovateli uplatňovat smluvní pokutu ve výši 0,2 % z ceny poskytovaných služeb za každý den prodlení.
(6) V případě provádění služby poddodavatelem, pro kterého objednatel neudělil souhlas, je-li souhlas v této smlouvě vyžadován, nebo poddodavatelem, který nebyl objednateli oznámen, je-li oznámení v této smlouvě vyžadováno, může po poskytovateli objednatel uplatňovat smluvní pokutu ve výši 40.000,- za poddodavatele.
(7) Poskytovatel je na základě ustanovení čl. IX. této smlouvy povinen zabezpečit prokazatelné proškolení všech pracovníků realizující služby s předpisy BOZP a požární ochrany. Pracovníkovi, který porušení předpisy BOZP nebo požární ochrany v prostorách objednatele, udělí poskytovatel pokutu ve výši 5.000,- Kč. Do doby zaplacení této pokuty poskytovatel nevpustí takového pracovníka do prostor objednatele.
(8) Smluvní pokuty jsou započitatelné vůči peněžitým závazkům souvisejících s touto smlouvou.
(9) Nároky na náhradu újmy nejsou dotčeny ani kompenzovány zaplacením sankcí dle této smlouvy.
(10) Je-li vůči smluvní straně uplatněna smluvní pokuta či úrok z prodlení podle tohoto článku, je taková smluvní strana povinna je uhradit.

XII.
Odstoupení od smlouvy

(1) Pro účely odstoupení od smlouvy se za podstatné porušení smlouvy považuje zejména:
- vadnost poskytovaných služeb již v průběhu jejich provádění, pokud poskytovatel na písemnou výzvu objednatele vady neodstraní ve lhůtě výzvou stanovené,
- prodlení poskytovatele se zahájením nebo dokončením poskytování služeb **o více než 2 pracovní dny**,
- **opakované (tj. nejméně 2x)** prodlení poskytovatele se zahájením nebo dokončením poskytování služeb spočívajících v poskytování podpory provozu systému vč. operativních služeb,
- nedostupnost podpory provozu nebo zajištění rozhraní mezi objednatelem a poskytovatelem pro operativní služby **delší než 24 hodin**,
- úpadek objednatele ve smyslu § 3 zák. č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů,
- zahájení insolvenčního řízení, ve kterém je poskytovatel v postavení dlužníka.

(2) Dojde-li k výše uvedenému porušení smlouvy, je příslušná smluvní strana oprávněna od smlouvy odstoupit. Odstoupení od smlouvy musí být učiněno písemnou formou. V takovém případě nastávají účinky odstoupení od smlouvy dnem, ve kterém smluvní straně dojde oznámení o odstoupení ve smyslu § 570 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Od smlouvy je

možné odstoupit jak bez zbytečného odkladu, tak i v případě, pokud důvod, pro který je odstupováno, stále přetrvává.

(3) Odstoupením od této smlouvy nezaniká vzájemná sankční odpovědnost stran ani povinnost k náhradě způsobené újmy.

XIII.
Důvěrnost informací

(1) Smluvní strany jsou si vědomy toho, že v rámci plnění smlouvy:
- si mohou vzájemně poskytnout informace, které budou považovány za důvěrné (dále důvěrné informace),
- mohou jejich zaměstnanci získat přístup k důvěrným informacím druhé strany.

(2) Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany. S výjimkou plnění této smlouvy, se obě strany zavazují nepublikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli splnit smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění smlouvy nebo uplatnění svých práv z této smlouvy.

(3) Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. například popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit újmu.

(4) Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.

(5) Ustanovení tohoto článku není dotčeno ukončením účinnosti smlouvy z jakéhokoliv důvodu a jeho účinnost skončí nejdříve pět (5) let po ukončení účinnosti této smlouvy.

XIV.
Závěrečná ustanovení

(1) Vztahy plynoucí z této smlouvy a vztahy neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

(2) Smluvní strany berou na vědomí, že společnost Brněnské komunikace a.s. je povinna dodržovat ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

(3) Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv postupem dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, a její zveřejnění zajistí objednatel.

(4) Žádná ze smluvních stran není oprávněna postoupit práva či pohledávky nebo převést závazky z této smlouvy vyplývající na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany. Práva i povinnosti ze smlouvy přecházejí na právní nástupce obou stran. Obě strany jsou povinny informovat se navzájem o takových změnách.

(5) Tuto smlouvu lze měnit pouze písemnou formou číslovanými dodatky podepsanými oběma smluvními stranami.

(6) Tato dohoda je vyhotovena ve dvou stejnopisech, z nichž po jednom obdrží každá ze smluvních stran.

(7) Smluvní strany prohlašují, že si tuto smlouvu přečetly, bezvýhradně souhlasí s jejím obsahem a že ji uzavírají ze své vážné a svobodné vůle, prosté omylu. Na důkaz toho připojují podpisy svých oprávněných zástupců.

(8) Nedílnou součástí této smlouvy je příloha č. 1.

Přílohy:
Příloha č. 1: Technická specifikace

Za objednatele:

V Brně dne 02. 05. 2022

[redacted]

Ing. Luděk Borový
generální ředitel

Za poskytovatele:

V Brně dne 20.4.2022

[redacted]

Pavel Kocour
Předseda představenstva

Příloha č. 1 – Technická specifikace

Systém dodaný poskytovatelem má níže požadované funkce, nejedná se o budoucí funkce plánovaných verzí software.

Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Nabízená hodnota
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
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	ANO
Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	ANO
Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému – uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	ANO
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

Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.	ANO
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
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
Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.	ANO
Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO
Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO
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
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

Systém provádí konsolidaci logů na interním úložišti logovacího systému.	ANO
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
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
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
Systém provádí automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy.	ANO
Systém podporuje nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.	ANO
V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	ANO
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	ANO
Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.	ANO
Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	ANO
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

Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO
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
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
Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB.	ANO
Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO
Monitoring stavu systému – upozornění při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	ANO
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
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
Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	ANO

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
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
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	
Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	ANO
HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	ANO
1 procesor, min. 16 jader, s podporou Hyper-Threadingu nebo Multi-Threadingu.	ANO
RAM Min. 64GB DDR-4.	ANO
Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	ANO
Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	ANO
Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci.	ANO
Větráky v systému musí být vyměnitelné za provozu a redundantní.	ANO
2x napájecí zdroje s redundancí napájení 1+1.	ANO
Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	ANO
Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ANO
Výkonnostní a SW parametry systému	
Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	ANO

Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	ANO
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
Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	ANO
Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	ANO
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat.	ANO
Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	ANO
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.	ANO

Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. Doložte odkazem na dokumentaci, jakým způsobem lze plnit textové tabulky prostřednictvím REST-API nabízeného systému.	ANO
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
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
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
Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – požadujeme podporu minimálně 2 nodů. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.	ANO
Dvounodový cluster se chová jako 1 celek.	ANO
V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.	ANO

V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	ANO
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
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
Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	ANO
Alerty	
Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO
Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO
Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO
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
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
V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	ANO
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	
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Tento agent musí současně podporovat jak monitoring interních Windows logů, tak monitoring textových souborových logů. Agenty musí být možné instalovat vzdáleně prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.	ANO
Podpora sběru z Microsoft prostředí musí být možná i prostřednictvím technologického standardu Open Source Elastic Search Beats, taktéž s centrálním managementem v konzoli dodaného systému pro Beats agenty a instalací agenta prostřednictvím Microsoft AD GPO. Doložte odkazem na dokumentaci, jakým způsobem se centrálně spravuji Windows agenti na bázi Open Source Elastic Search Beats.	ANO
Používaní agenti pro sběr dat podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.	ANO
Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně Windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. 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
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.	ANO
Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše.	ANO
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
Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO

Počet instalací Windows agenta by neměl být licenčně a časově omezen. Pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 350 na dobu předpokládané morální životnosti produktu – 7 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit, že systém výkonnostně splňuje tento požadavek. Jedná se o klíčovou funkci, proto budeme před uzavřením smlouvy požadovat předvedení požadovaných funkcí, stability i výkonnostní kapacity nabízeného systému pro sběr logů z prostředí Microsoft.	ANO
Podpora pro sběr událostí z poboček	
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
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
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
Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO
Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO
Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO
Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO
Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO
Vysoká dostupnost, SW Podpora a záruka na hardware	
Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.	ANO
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
Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO

SW – podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW minimálně 3x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO

Obecné požadavky na služby podpory provozu

V rámci provozních činností prováděných v prostředí Objednatele jsou vyžadovány požadavky podle následující tabulky:

Požadavek	Kritérium
Přístup k podpoře provozu Log management službě	HotLine/Ticket systém
Přístup k podpoře Incident Response	Telefon/E-mail
Dostupnost podpory provozu	5 x 16 (Po-Pá 6-22 CET)
Reakční čas na změnu konfigurace mimo Incident Response	1 pracovní den
Čas na stabilizaci Log management systému	do 45 minut
Nezbytný počet specialistů dodavatele	2 osoby
Požadovaná alokace času specialistů na 1 rok pro Configuration & Change management	10 hodin
Aktualizace nových verzí Log managementu	Vyžadováno v rámci Řízení změn objednatelem
Proxylaxe	Periodická kontrola souladu nastavení Log management komponent. Průběžné sledování provozu smluvního zařízení klienta. V případě provozní anomálie neprodlené posouzení její relevance a závažnosti.
Configuration & Change management	Zapracování změn podle požadavků objednatele nebo podle požadavků či best-practice výrobce Log management nástroje.

Obecné požadavky na Operativní služby

Pro zajištění služby *Detekce anomálií, včasné výstrahy a reakce na nestandardní situace v provozu* jsou vyžadovány požadavky podle následující tabulky:

Požadavek	Kritérium
Zajištění rozhraní mezi Objednatelem a Provozovatelem služby	Přijetí hovoru na ServiceDesk provozovatele služby.

	Možnost on-line vložení Požadavku/Ticketu na ServiceDesk provozovatele služby.
Služba Monitoringu a detekce - Zajištění Operátorské úrovně – Layer 0	Průběžné sledování provozu prostředí objednatele. Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. 2x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti. Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému objednatele na analytického specialistu dodavatele. 1x za měsíc report provozu a kvality prostředí. Dostupnost Operátorské úrovně v režimu 5 x 16 (Po-Pá 6-22 CET).
Služba včasné výstrahy a reakce na nestandardní situace v provozu Log management - Incident Response (CERT) – Layer-3	**Analyze** - Zpracování analytických scénářů na aktuální kybernetické hrozby. **Detection** - Posouzení eskalovaného problému objednatele analytickým specialistou. **Event & Incident management** - Detekce a vyhodnocení závažnosti identifikovaných anomálií v prostředí Log managementu (např. zvýšení trendu generování log záznamů, změna struktury log záznamů [nový log záznam, změna lokalizace jazyka zpráv, ...],....) **Emergency** - Posouzení a případná eskalace nestandardní situace v provozu objednatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.
Reakční čas na mimořádnou událost	do 30 minut
Čas na stabilizaci a na protiopatření vůči identifikované anomální situaci	do 45 minut od identifikace anomální situace
Režim služby pro Log management systém	Je vyžadován režim 5 x 16 (Po-Pá 6-22 CET).