

KUPNÍ SMLOUVA

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

I. Smluvní strany

Prodávající:

Název: CompuNet s. r. o.
Sídlo firmy: Zubatého 295/5, 150 00 Praha 5
Zastoupená: Ing. Pavlem Pikhartem, jednatelem
IČO: 276 08 514
DIČ: CZ27608514
Bankovní spojení: Komerční banka a.s., pobočka Praha 5
Číslo účtu:
Telefon:

Zapsána v obchodním rejstříku vedeném u Krajského soudu v Praze, oddíl C, vložka 118594

Kupující:

Název: Puncovní úřad
Sídlo firmy: Kozí 748/4, 110 00 Praha – Staré Město
Zastoupený: Ing. Jana Davidková, předsedkyně Puncovního úřadu
IČ: 00002542
Bankovní spojení: Česká národní banka
Číslo účtu:
Kontaktní osoba: Jiří Šnajdr
Telefon:
Email:

II. Předmět plnění smlouvy

1. Předmětem plnění této smlouvy je dodávka a implementace centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů a aplikací zadavatele dle specifikace uvedené v Příloze č. 1 (dále jen „předmět smlouvy“ nebo „zboží“) ve prospěch kupujícího a za úhradu kupní ceny, a to na základě realizace veřejné zakázky malého rozsahu ve smyslu ustanovení § 31 zákona č. 134/2016 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, která proběhla prostřednictvím elektronického tržiště č. T004/18V/00006979.
2. Součástí předmětu plnění této smlouvy je rovněž předání dále uvedených dokladů:
 - a. Předávacího protokolu ke zboží
 - b. Záručních listů na jednotlivé komponenty dodávky zboží
 - c. Originálního příslušenství dodávaného v originálním balení výrobce k tomuto zboží
 - d. Technické dokumentace zboží v rozsahu dodávaném výrobcem zboží

III. Kupní cena

1. Kupní cena za dodávané zboží je stanovena dohodou obou smluvních stran této smlouvy a činí:

485 000,- Kč bez DPH,

(slovy: čtyři sta osmdesát pět tisíc korun českých),

kdy DPH ve výši 21% ceny bez DPH činí:

101 850,- Kč

(slovy: jedno sto jedna tisíc osm set padesát korun českých),

tj. celková cena činí:

586 850,- Kč s DPH,

(slovy: pět set osmdesát šest tisíc osm set padesát korun českých).

2. Kupní cena dle článku III. odstavce 1. této smlouvy zahrnuje: veškeré účelně vynaložené náklady prodávajícího spojené s koupí zboží ze strany kupujícího (dopravu do místa plnění, obaly a dokumentaci související s dodávkou zboží) včetně recyklačních poplatků.

IV. Místo a způsob dodání

1. Prodávající dodá předmět smlouvy do sídla kupujícího:

Kozí 748/4
110 00 Praha 1

do rukou přebírající osoby, (Jiří Šnajdr, tel.: , email:),
jakožto osoby určené k převzetí zboží za kupujícího.

V. Dodací podmínky

1. Prodávající je povinen dodat zboží dle čl. II. této smlouvy do 45 pracovních dní od data nabytí účinnosti této smlouvy.
2. Po této době může prodávající dodat zboží jen po předchozím písemném (e-mailovém), souhlasu kupujícího.
3. Prodávající nebude plnit tuto smlouvu po částech.
4. Kupující převezme od prodávajícího zboží splňující veškeré podmínky stanovené v této smlouvě.
5. Kupující není povinen převzít zboží, které vykazuje k okamžiku zamýšleného převzetí vady. V takovém případě o zjištěných vadách zboží vyhotoví zástupci smluvních stran ihned po odmítnutí zamýšleného převzetí zboží písemný zápis, který potvrdí svým vlastnoručním podpisem. Prodávající je v tomto případě povinen dodat kupujícímu nové a bezvadné zboží podle této smlouvy, a to formou náhradního plnění dodávky zboží ve lhůtě 5 pracovních dní ode dne odmítnutí zamýšleného převzetí zboží.

Sjednaná doba dodání zboží podle článku V. odst. 1 této smlouvy není tímto odmítnutím převzetí zboží nijak dotčena co do práva kupujícího na uplatnění sankce ve smyslu čl. VIII odst. 1 této smlouvy.

VI. Platební podmínky

1. Daňový doklad (faktura) na cenu dle čl. III této smlouvy bude prodávajícím vystaven na kupujícího po řádně poskytnutém plnění nebo náhradním plnění podle čl. V. odst. 1 a 5 této smlouvy. Daňový doklad musí obsahovat náležitosti dle příslušných účinných právních předpisů, zejména dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a § 435 občanského zákoníku.
2. Kupující je oprávněn fakturu do data splatnosti vrátit, pokud tato obsahuje nesprávné cenové údaje nebo pokud nemá náležitosti podle čl. VI. odst. 1 této smlouvy, popřípadě pokud předmět plnění neobsahuje některou z dohodnutých náležitostí podle této smlouvy.
3. Kupující je povinen v případě potvrzeného převzetí kompletní dodávky předmětu plnění smlouvy zaplatit fakturu do 14 dnů od jejího doručení. V případě oprávněného vrácení faktury ve smyslu čl. VI. odst. 2 této smlouvy se kupující nemůže ocitnout v prodlení se zaplacením částky fakturované oprávněně vrácenou fakturou, prodávající v takovém případě není oprávněn přistoupit k uplatnění sankce ve smyslu čl. VIII. odst. 2 této smlouvy. V případě oprávněného vrácení faktury se okamžikem jejího vrácení prodávajícímu přerušuje lhůta splatnosti vrácené faktury. Doručením nové faktury, obsahující veškeré náležitosti ve smyslu čl. VI. odst. 1 této smlouvy, kupujícímu, počíná běžet nová 14 denní lhůta splatnosti nové faktury.
4. Prodávající může zaslat fakturu v papírové formě na adresu Kozí 748/4, 110 00 Praha – Staré Město nebo elektronicky podepsanou kvalifikovaným certifikátem na e-mail
5. Vlastnické právo ke zboží přechází na kupujícího z prodávajícího úplným zaplacením kupní ceny zboží dle této smlouvy.

VII. Záruka

1. Prodávající prohlašuje, že zaručuje dohodnuté vlastnosti zboží podle záručních podmínek, které jsou nedílnou součástí zboží, a to po dobu záruční doby vyznačené na faktuře nebo na dodacím listu.
2. Záruční doba je stanovena na 36 kalendářních měsíců na hmotné části dodávky a počíná běžet dnem dodání a převzetí zboží.
3. Záruční doba neběží po dobu trvání případné vady, která brání užívání zboží k účelu, ke kterému jej kupující od prodávajícího zakoupil.
4. Kupující má právo vyžadovat po prodávajícím odstranění závady zboží kdykoliv během záruční doby poskytnuté mu prodávajícím na zboží. Oznamení o vadách zboží může být učiněno ze strany kupujícího jakoukoliv formou, včetně telefonické a musí

být následně potvrzeno bez zbytečného odkladu ze strany prodávajícího písemnou formou (např. faxem, dopisem, prostřednictvím elektronické pošty...), přičemž se uvede výstižný popis závady zboží a jméno oznamovatele výskytu vady na zboží za stranu kupujícího. Přijetí oznámení o vadách potvrdí prodávající kupujícímu telefonicky, dopisem, faxem, prostřednictvím elektronické pošty.

5. Prodávající neodpovídá kupujícímu za závady na zboží způsobené u kupujícího živelnou pohromou, mechanickým poškozením nebo neodborným zásahem ze strany kupujícího nebo třetí osoby.

VIII. Smluvní pokuty a sankce

1. Nedodá-li prodávající zboží ve lhůtách uvedených v čl. V odst. 1 této smlouvy, vzniká kupujícímu právo na smluvní pokutu ve výši 0,05 % z ceny nedodaného zboží, včetně DPH, za každý den prodlení. Smluvní pokuta je splatná do 30 dnů od doručení faktury na smluvní pokutu s výzvou kupujícího prodávajícímu k zaplacení smluvní pokuty.
2. V případě prodlení kupujícího s úhradou daňového dokladu (faktury) vzniká prodávajícímu právo na úrok z prodlení ve výši 0,05 % z ceny dodaného a kupujícím nezaplaceného zboží, včetně DPH, za každý den prodlení. Povinnost zaplatit úrok z prodlení vzniká kupujícímu do 30 dnů od doručení faktury na úrok z prodlení s výzvou prodávajícího kupujícímu k zaplacení úroku z prodlení.
3. Obě smluvní strany se zavazují před uplatněním nároku na smluvní pokutu nebo na úrok z prodlení vyzvat písemně druhou smluvní stranu k podání vysvětlení vzniklé situace.
4. Zaplacení smluvní pokuty nezavazuje prodávajícího povinnosti splnit závazek k řádné dodávce zboží stanovený touto smlouvou.

IX. Závěrečná ustanovení

1. Smluvní strany mohou od smlouvy odstoupit v souladu s § 2001 a násl. občanského zákoníku.
2. Tato smlouva může být měněna nebo doplňována jen písemnými, očíslovanými dodatky. Za písemnou formu nebude pro tento účel považována výměna e-mailových či jiných elektronických zpráv. Kupující je oprávněn namítnout neplatnost smlouvy či jejího dodatku z důvodu nedodržení formy kdykoli, a to i když již bylo započato s plněním.
3. Smluvní vztahy výslovně neupravené v této smlouvě se řídí občanským zákoníkem a právními předpisy souvisejícími.
4. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá smluvní strana obdrží po jednom vyhotovení.
5. Obě smluvní strany prohlašují, že se měly možnost seznámit se zněním této smlouvy, obsahu smlouvy rozumí a chtějí jím být vázány. Žádný projev stran učiněný při

jednání o této smlouvě ani projev učiněný po uzavření této smlouvy nesmí být vykládán v rozporu s výslovným ustanovením této smlouvy.

6. Tuto smlouvu nelze postoupit bez souhlasu druhé smluvní strany. Prodávající není oprávněn postoupit jakékoli pohledávky vyplývající z této smlouvy vůči kupujícímu na kteroukoli třetí osobu bez předchozího písemného souhlasu kupujícího.
7. Smlouva nabývá platnosti, jakož i účinnosti podpisem Smlouvy tou smluvní stranou, která ji podepíše jako poslední.
8. Smlouva nabývá platnosti, jakož i účinnosti podpisem Smlouvy tou smluvní stranou, která ji podepíše jako poslední.

Příloha č. 1: Dodávka, implementace a podpora centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů a aplikací zadavatele

V Praze, dne: 30.5.2018

V Praze dne: 31.5.2018

.....
prodávající
Ing. Pavel Pikhart,
jednatel

.....
kupující
Ing. Jana Davídková,
předsedkyně Řídicího úřadu

Příloha č. 1: Dodávka, implementace a podpora centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů a aplikací zadavatele

PN	Popis	ks	Cena za kus	Cena celkem
LOGmanager "Malý" - 1 x CPU / 10 x Core Xeon, RAM 64GB, 4 x 4TB = 16TB, RAID 5 = 12TB, V ceně 3-letý Care Pack NBD - podpora na HW!				385 000 Kč
LGM-16TB	LOGmanager vč. podpory na 1 rok	1	295 000 Kč	295 000 Kč
LGM-rnwl-maly-1y	1 rok (SW upgrade) + 5hod tel. podpora / rok	2	45 000 Kč	90 000 Kč
Ostatní				100 000 Kč
Práce	Implementace vč. konfigurace sledovaných zařízení	1	75 000 Kč	75 000 Kč
Školení	Zaškolení obsluhy LOGmanageru	1	25 000 Kč	25 000 Kč

Ce kem bez DPH	485 000 Kč
DPH (21%)	101 850 Kč
Ce kem vč. DPH	586 850 Kč

Dodávka a implementace centrálního úložiště logů pro sběr bezpečnostních událostí z kritických systémů a aplikací zadavatele

Předmět zakázky:

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. Nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů.

Systém musí umožňovat tvorbu uživatelsky definovaných parserů bez účasti výrobce nebo dodavatele a dokumentace v českém jazyce musí poskytnout jednoznačný návod, jak takovéto parsery vytvářet.

Technická specifikace

Číslo	Popis	Splňuje
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	
1	Systém pracuje jako appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.	Ano/Ne
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobcí aplikací, operačních systémů a síťového hardware.	Ano/Ne
3	Systém umožňuje dopsání parseru 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 psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce.	Ano/Ne

4	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožňovat příjem logů i na uživatelsky definovaných UDP a TPC portech. 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.	Ano/Ne
5	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/Ne
6	Všechny pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano/Ne
7	Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159.	Ano/Ne
8	Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	Ano/Ne
9	Systém provádí konsolidaci logů na centrálním místě.	Ano/Ne
10	Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.	Ano/Ne
11	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/Ne
12	Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období.	Ano/Ne
13	Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.	Ano/Ne
14	Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám.	Ano/Ne
15	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/Ne
16	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.	Ano/Ne
17	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 ani čestným prohlášením.	Ano/Ne
18	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	Ano/Ne
19	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/Ne
20	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano/Ne
21	Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.	Ano/Ne
22	Konfigurační a Systémové rozhraní a dokumentace musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce.	Ano/Ne
23	Systém nabízí kapacitní i výkonovou škálovatelnost.	Ano/Ne

24	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB.	Ano/Ne
25	Požadujeme, aby ze systému bylo možné vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	Ano/Ne
26	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	Ano/Ne
27	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.	Ano/Ne
28	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/Ne
29	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/Ne
30	Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.	Ano/Ne
31	Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes WMI protokol neumožňuje monitorovat textové logy.	Ano/Ne
32	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze.	Ano/Ne
	Minimální HW parametry požadovaného systému	
33	Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	Ano/Ne
34	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.	Ano/Ne
35	1 procesor (min. 10 jader), podpora HyperThreadingu.	Ano/Ne
36	Min. 64GB DDR-4.	Ano/Ne
37	Minimálně 12TB pro integrovanou databázi podporovanou HW akcelерованým SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	Ano/Ne
38	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/s.	Ano/Ne
39	Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.	Ano/Ne
40	Větráky v systému musí být vyměnitelné za provozu a redundantní.	Ano/Ne
41	2x napájecí zdroje s redundancí napájení 1+1.	Ano/Ne
42	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	Ano/Ne
43	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	Ano/Ne
	Výkonnostní a SW parametry systému	

44	System funguje formou appliance (všechny části systému je možné nastavit v centrální správčovské konzoli - viz bod 29, není nutné editovat žádné konfigurační soubory včetně IP adresace systému).	Ano/ Ne
45	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správčovskou konzoli (viz bod 29).	Ano/ Ne
46	System musí podporovat downgrade, pro případ problémů s novou verzí systému po upgrade.	Ano/ Ne
47	Průměrný trvalý příjem min. 2 tis událostí / s.	Ano/ Ne
48	Špičkový příjem 4 tis událostí / s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později.	Ano/ Ne
49	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 80GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat.	Ano/ Ne
50	Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správčovské webové konzoli (viz bod 29). 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/ Ne
51	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeolIP informace a identifikace výrobce zařízení podle MAC adresy.	Ano/ Ne
52	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení.	Ano/ Ne
53	V centrální správčovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.	Ano/ Ne
54	V centrální správčovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	Ano/ Ne
55	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/ Ne
56	Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active / active.	Ano/ Ne
57	Vícenodový systém se chová jako 1 celek.	Ano/ Ne
58	V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	Ano/ Ne
59	Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru.	Ano/ Ne
60	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/ Ne
61	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.	Ano/ Ne
	Alerty	
62	System je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.	Ano/ Ne
63	Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události.	Ano/ Ne
64	Předpřipravené sety/vzory alertů výrobcem.	Ano/ Ne
65	Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	Ano/ Ne

66	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol.	Ano/Ne
67	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/Ne
Sběr událostí z Microsoft prostředí		
68	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.	Ano/Ne
69	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	Ano/Ne
70	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správčovské konzole z bodu 29.	Ano/Ne
71	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správčovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	Ano/Ne
72	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy.	Ano/Ne
73	Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	Ano/Ne
74	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	Ano/Ne
75	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	Ano/Ne
76	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.	Ano/Ne
77	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	Ano/Ne
78	Počet instalací Windows agenta nesmí být licenčně omezen. (případně požadujeme licenci na 1000 systémů.)	Ano/Ne
Podpora pro sběr událostí z poboček		
79	Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	Ano/Ne
80	Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat.	Ano/Ne
81	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášet data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	Ano/Ne
82	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	Ano/Ne
83	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	Ano/Ne
84	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí /s. a to i v trvalé zátěži.	Ano/Ne
85	Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.	Ano/Ne
86	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	Ano/Ne
87	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	Ano/Ne

SW Podpora a záruka na hardware		
88	HW - Požadovaná min. 3 letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	Ano/Ne
89	SW - Podpora výrobce na aktualizaci systému a parserů na 3 roky. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonická a emailová podpora s diagnostikou vzdáleným přístupem.	Ano/Ne

Ověření funkčních vlastností

Zadavatel po rozhodnutí o výběru nejvhodnější nabídky vyzve vybraného Uchazeče k zapůjčení nabízeného systému pro účely testování a ověření požadovaných funkčních vlastností. Uchazeč je povinen doručit testovací vzorky na Místo plnění do deseti (10) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný Uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně 14 kalendářních dnů. Uchazeč v rámci testovacího provozu provede tyto práce:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele
- Konfigurace systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného systému
- Ověření funkčních a výkonových parametrů Windows agenta – 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
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz Technická specifikace, odstavec SW parametry
- Značkování událostí, vytvoření Alertu dle zadání Zadavatele – viz Technická specifikace, odstavec SW parametry a odstavec Alerty (příklad: pošli alert jen v případě, že se událost stala na kritickém Windows serveru, který běží v lokalitě Praha)
- Odeslat událost, která vyvolala alert na externí syslog server přes TCP protokol
- Představení plnohodnotné dokumentace pro nabízený systém v českém jazyce

Testování bude provádět dodavatel za účasti zástupců zadavatele, který mu poskytne potřebnou součinnost. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou testovací vzorky Uchazeči vráceny (Uchazeč si vyzvedne vzorky na vlastní náklady v Místě plnění).

Testovací provoz bude zakončen akceptací a bude vyhotoven Akceptační protokol. V případě, že testovaný systém neprojde úspěšným otestováním, neuzavře Zadavatel s takovým uchazečem smlouvu a vyzve k dodání testovacích vzorků Uchazeče, který se v hodnocení nabídek umístil jako další v pořadí.

Akceptační testy

Minimální rozsah akceptačních testů:

- Detailní parserování logů zařízení a systémů uvedených v požadavcích výběrového řízení.
- Prohledání 4.000.000 (čtyřmilióny) záznamů, zobrazení histogramu a TOP hodnot z osmi rozparovaných polí nejdéle za 10sec.
- Průměrný příjem min 2 tis událostí/s. Ověření v 10minutovém intervalu pomocí generátoru událostí.

- Špičkový příjem min 4 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 – viz. Technická specifikace, odstavec „Sběr událostí z Microsoft prostředí“
- Simulace provozu na pobočce a ověření funkčních vlastností řešení pro vzdálený sběr událostí na pobočkách z UDP zdroje a Windows Agentu. Výkonové testy řešení pro vzdálený sběr událostí s příjmem minimálně 3 tis událostí/s.
- 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 Alertu dle zadání Zadavatele - viz. Technická specifikace, odstavec SW parametry a odstavec Alerty (příklad: pošli alert jen v případě, že se událost stala na kritickém Windows serveru, který běží v lokalitě Praha) 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.