TSKRP00B58T8

KUPNÍ SMLOUVA

uzavřená podle § 2079 a násl., zákona č. [redacted] Sb., občanský zákoník,

číslo smlouvy Kupujícího: 4/20/3254/039
číslo smlouvy Prodávajícího: SMLK/KA/16230

I.
Smluvní strany

1. **Kupující:** **Technická správa komunikací hl. m. Prahy, a.s.**
Řásnovka 770/8, 110 00 Praha 1
IČO: 03447286
DIČ: CZ 03447286
Zapsána v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 20059
Bankovní spojení: PPF banka a.s.
Číslo účtu: [redacted]
zastoupena: Mgr. Jozefem Sinčákem, MBA, předsedou představenstva
Prof. Ing. Karlem Pospíšilem, Ph.D., místopředsedou představenstva
PhDr. Filipem Hájkem, členem představenstva
Ing. Martinem Pípou, členem představenstva

Při podpisu Smlouvy a veškerých jejich Dodatků jsou oprávněni zastupovat Kupujícího dva členové představenstva společně, z nichž nejméně jeden musí být předsedou anebo místopředsedou představenstva. Při podpisu Smlouvy s hodnotou plnění do 2 mil. Kč je oprávněn zastupovat Kupujícího v souladu s Maticí odpovědnosti na základě pověření uděleného představenstvem, Michal Berounský, ředitel úseku informatiky.

Osoby oprávněné k jednání ve věcech technických:

Michal Berounský, ředitel úseku informatiky
Jiří Peterka, specialista IT bezpečnosti a GDPR

(dále jen „**Kupující**")

2. **Prodávající:** **COMTESYS, spol. s r.o.**
Sídlo: Pod Pramenem 1633/3, 1400 Praha 4
IČO: 26490234
DIČ: CZ26490234
zapsaná v obchodním rejstříku vedeném: Městským soudem v Praze, spis. Zn. C 85526
Bankovní spojení: ČSOB, a.s.
Číslo účtu: [redacted]
Zastoupený: Ing. Martinem Vobořilem, jednatelem společnosti
k podpisu předávacího protokolu oprávněn: Roman Koutecký, obchodní ředitel
zastoupený ve věcech technických: Miloslav Celner, technický ředitel
e-mail pro účely fakturace: [redacted]

(dále jen „**Prodávající**")

Smluvní strany dnešního dne uzavírají v souladu s § 2079 a násl. zákona č. [redacted] Sb., občanský zákoník (dále jen „**Občanský zákoník**") tuto kupní smlouvu (dále jen „**Smlouva**") na základě Prodávajícím předložené nabídky ve veřejné zakázce malého rozsahu **„Dodávka a implementace systému pro centralizované ukládání a správu logů pro TSK hl. m. Prahy, a.s."**, realizované Kupujícím dle zákona č. [redacted] Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

II.

Předmět smlouvy

1. Předmětem Smlouvy je **„Dodávka a implementace systému pro centralizované ukládání a správu logů"** dle požadavku Kupujícího.
   Jedná se o dodání a implementaci centrálního úložiště pro sběr a analýzu logů (SEM/SIEM řešení) umožňujícího následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací (dále jen „systém").

   Povinné parametry:

   Systém musí zachovávat originál logů za účelem umožnění bezpečnostního auditu dle příslušné legislativy, zejména zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v platném a účinném znění.

   Systém musí být v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat za účelem možnosti zjištění informací o bezpečnostních incidentech, provozních stavech a případných závadách v informačních technologiích v reálném čase i do minulosti nejméně jeden rok zpět. Dále musí být schopný generovat reporty o aktivitách informačních systémů, aplikací i uživatelů, včetně auditních reportů na vyžádání nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

   Součástí dodávky bude úplná a podrobná dokumentace k systému i všem návazným komponentům v českém jazyce, obsahem i kvalitou srovnatelná s aktuální dokumentací v anglickém či jiném jazyce. Dodaný systém musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Musí poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.

   Podrobnější popis předmětu plnění je uveden v příloze č. 1 Technická specifikace a v příloze č. 2 Seznam povinně podporovaných logů.

   (dále jen „**Předmět koupě**").

2. Popis Předmětu koupě je specifikován v předchozím odstavci této Smlouvy, v Příloze č. 1 a 2 této Smlouvy (dále jen Příloha č. 1 a č. 2).
3. Prodávající se zavazuje řádně a včas, v souladu se specifikací obsaženou v Příloze č. 1 a 2 této Smlouvy a za podmínek stanovených touto Smlouvou, dodat Kupujícímu Předmět koupě a provést implementaci a Kupující se zavazuje Předmět koupě, vč. provedené implementace převzít a zaplatit Prodávajícímu dohodnutou kupní cenu.
4. Prodávající prohlašuje, že se v plném rozsahu seznámil s rozsahem a povahou Předmětu koupě, a že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k jeho dodávce a implementaci.
5. Prodávající se při dodávce a implementaci Předmětu koupě bude řídit výchozími podklady a podmínkami Kupujícího a podklady odevzdanými ke dni uzavření Smlouvy.
6. Kupující se zavazuje, že na vyzvání Prodávajícího mu bez zbytečného odkladu poskytne další vyjádření, stanoviska, informace, případně doplnění podkladů, jejichž potřeba vznikne v průběhu dodávky či implementace Předmětu koupě a z této Smlouvy nebo z povahy věci nevyplývá, že Prodávající je povinen si je opatřit sám.
7. Předmět koupě bude dodán a implementován v souladu s podklady a zadáním předaným Kupujícím, kterými jsou parametry uvedené v Příloze č. 1 a 2 Smlouvy. Jakékoliv změny oproti sjednanému Předmětu koupě, jeho rozsahu a termínu dokončení dodávky a implementace, které vyplynou z dodatečných požadavků Kupujícího nebo ze změny jím předaných podkladů, z důvodu vyšší moci či nepředpokládaných překážek neležících na straně Prodávajícího, budou řešeny formou dodatků k této Smlouvě.

V těchto dodatcích smluvní strany dohodnou odpovídající změnu Předmětu koupě, doby plnění dodávky a implementace a ceny za Předmět koupě.

8. Smluvní strany se dohodly, že kontaktními osobami, odpovědnými ve věcech technických souvisejících s Předmětem koupě jsou:
   a) za Kupujícího: Jiří Peterka, tel.: [redacted]
      Michal Berounský, tel.: [redacted]
   b) za Prodávajícího: Jakub Machát. Tel.: [redacted]

III.
Místo dodání a implementace

1. Místem dodání a implementace Předmětu koupě je sídlo Kupujícího: Řásnovka 770/8, 110 00 Praha 1. Předání a implementace Předmětu koupě bude potvrzeno předávacím protokolem podepsaným oprávněnými osobami obou smluvních stran.
2. Prodávající se zavazuje nejpozději 1 pracovní den před dnem dodání Předmětu koupě oznámit tuto skutečnost Kupujícímu a dohodnout s ním technické podrobnosti dodání a následné implementace Předmětu koupě.

IV.
Termín plnění

1. Termín zahájení plnění: na výzvu Kupujícího, nejdříve však po zveřejnění této Smlouvy v registru smluv
2. Termín dodání HW vč. implementace: do 40 dnů od výzvy Kupujícího

V.
Kupní cena

1. Celková kupní cena Předmětu koupě sjednaná dle odst. 2 tohoto článku je cenou nejvýše přípustnou.

2. **Cena za Předmět koupě bez DPH:** **1.190.400,- Kč**
   DPH 21%: **249.984,- Kč**
   Cena za Předmět koupě včetně DPH: **1.440.384,- Kč**

   Podrobná specifikace ceny je uvedena v příloze č. 3 této Smlouvy.

3. Cena Předmětu koupě pokrývá veškeré náklady Prodávajícího souvisejícími s dodáním a implementací Předmětu koupě, veškeré práce a dodávky, poplatky, platby a jiné náklady nezbytné pro řádnou a úplnou realizaci sjednaného rozsahu Předmětu koupě.

VI.
Platební podmínky

1. Veškeré daňové doklady musejí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že daňové doklady nebudou mít odpovídající náležitosti, je Kupující oprávněn zaslat je ve lhůtě splatnosti zpět Prodávajícímu k doplnění, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených dokladů.
2. Fakturace bude provedena jednorázově. Přílohou faktury bude předávací protokol podepsaný oprávněnými osobami obou smluvních stran a další požadované doklady (záruční list, certifikát, atd.) budou neprodleně předány Kupujícímu.
3. Splatnost faktury je stanovena na 30 dní po jejím doručení Kupujícímu a bude vystavena do 5 pracovních

dnů po převzetí dodaného Předmětu koupě a jeho řádné implementaci. Zálohy nebudou poskytovány. Faktura vystavovaná Prodávajícím bude obsahovat text následujícího znění: **„Dodávka a implementace systému pro centralizované ukládání a správu logů pro TSK hl. m. Prahy, a.s.“.**

4. Jako odběratel bude uvedeno ve faktuře:

Technická správa komunikací hl. m. Prahy, a.s.
IČO: 03447286
DIČ: CZ03447286
Řásnovka 770/8
110 00 Praha 1
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 20059

Smluvní strany souhlasí s použitím faktur vystavených na základě Smlouvy výhradně v elektronické podobě (faktura má elektronickou podobu tehdy, pokud je vystavena a obdržena elektronicky) - dále jen „Elektronická faktura“. Smluvní strany sjednávají, že věrohodnost původu faktury v elektronické podobě a neporušenost jejího obsahu bude zajištěna v souladu s platnou právní úpravou. Prodávající je povinen doručit Kupujícímu fakturu elektronicky, a to výlučně e-mailem na e-mailovou adresu: [redacted] Zaslání Elektronické faktury Prodávajícím na jinou e-mailovou adresu než uvedenou v předchozí větě je neúčinné. K odeslání Elektronické faktury je Prodávající povinen využít pouze e-mailovou adresu Prodávajícího uvedenou pro tento účel ve Smlouvě, jinak je zaslání Elektronické faktury neúčinné s výjimkou, budou-li průvodní e-mail k Elektronické faktuře či Elektronická faktura opatřeny zaručeným elektronickým podpisem, případně zaručenou elektronickou pečetí Prodávajícího. Elektronická faktura musí být Kupujícímu zaslána vždy ve formátu PDF a zároveň i ISDOC (ISDOCX), je-li to možné. Přílohy Elektronické faktury, které nejsou součástí daňového dokladu, budou zasílány Kupujícímu pouze ve formátech RTF, PDF, JPG, DOC, DOCx, XLS, XLSx. Elektronická faktura musí být opatřena zaručeným elektronickým podpisem, případně zaručenou elektronickou pečetí, obojí založené na kvalifikovaném certifikátu ve smyslu zákona č. [redacted] Sb. o službách vytvářejících důvěru pro elektronické transakce podpisu, ve znění pozdějších předpisů, kvalifikovaný certifikát musí být vydán jedním z Ministerstvem vnitra ČR akreditovaných poskytovatelů certifikačních služeb. Není-li Elektronická faktura opatřena zaručeným elektronickým podpisem, případně zaručenou elektronickou pečetí ve smyslu předchozí věty nebo není-li takto opatřen alespoň průvodní e-mail k Elektronické faktuře, musí být Elektronická faktura odeslána e-mailem výhradně z e-mailové adresy Prodávajícího uvedené pro tento účel ve Smlouvě, jehož přílohou je Elektronická faktura. Elektronická faktura bude vyhotovena v četnosti 1 e-mail - 1 Elektronická faktura v samostatném souboru a její přílohy v samostatném souboru (souborech). V případě, kdy bude zaslána Kupujícímu Elektronická faktura, zavazuje se Prodávající nezasílat stejnou fakturu duplicitně v listinné podobě. Prodávající je povinen odeslat Kupujícímu fakturu shora uvedeným postupem, nejpozději do pěti (5) pracovních dnů od vzniku jeho nároku na zaplacení Ceny.

VII.
Záruka

Obě smluvní strany se dohodly s odkazem na § 2095 a násl. Občanského zákoníku na níže uvedených vlastnostech Předmětu koupě

1. Prodávající poskytne záruční dobu na dodávku a implementaci v délce 60 měsíců (podmínky záručního servisu jsou uvedeny v Technické specifikaci, která tvoří Přílohu č. 1 Smlouvy).
2. Prodávající zaručuje Kupujícímu, že Předmět koupě odevzdaný v souladu s touto smlouvou:

a) je nový a nepoužitý;
b) je plně funkční a má obvyklé technické vlastnosti, odpovídající technickým údajům výrobce zboží
c) je použitelný v České republice. V této souvislosti Prodávající zejména zaručuje Kupujícímu, že Předmět koupě získal veškerá nezbytná osvědčení pro užití v České republice, pokud je takové osvědčení dle právního řádu České republiky vyžadováno. Prodávající předá kopie těchto osvědčení Kupujícímu při

odevzdání zboží;

d) má jakost a provedení stanovené v této Smlouvě;
e) je odevzdán v druhu a množství uvedeném ve Smlouvě;
f) je bez materiálových, konstrukčních, výrobních a vzhledových či jiných vad;
g) je bez právních vad, zejména že Předmět koupě není zatížen zástavními, předkupními, nájemními či jinými právy třetích osob. Prodávající je oprávněn převést bez dalšího vlastnické právo k Předmětu koupě na Kupujícího a Kupující je oprávněn Předmět koupě užívat a předat ho dále třetím osobám;
h) je bezpečný z hlediska českých právních předpisů;

3. Bude-li mít předaný Předmět koupě vady, sjednávají smluvní strany právo Kupujícího požadovat bezplatné odstranění vady, pokud je toto proveditelné. Není-li odstranění vady možné, má Kupující právo na slevu z ceny, příp. má právo od Smlouvy odstoupit, a to dle volby Kupujícího. Tímto ujednáním není dotčena povinnost Prodávajícího nahradit Kupujícímu veškerou vzniklou škodu.
4. Prodávající se zavazuje začít s odstraňováním vady na Předmětu koupě bez prodlení po nahlášení, nejpozději však do 24 hodin od nahlášení vady Kupujícím. Prodávající se zavazuje odstranit nahlášenou vadu bez zbytečného odkladu, nejpozději však do 5 (pěti) dnů od nahlášení této vady Kupujícím, nebude-li mezi smluvními stranami písemně dohodnuto jinak.
5. Prodávající prohlašuje, že hlášení vad je možné provádět v pracovních dnech od 8:00 do 17:00 hod., a to na kontaktech uvedených níže. Smluvní strany se dohodly, že Kupující bude nahlašovat vady Předmětu koupě u Prodávajícího, a to bez zbytečného odkladu po jejich zjištění. Při nahlášení vad budou tyto vady popsány či bude uvedeno, jak se projevují.

   Kontaktní údaje Prodávajícího pro nahlášení vad:
   adresa: [redacted]

6. Kontaktní údaje dle předchozího odstavce Smlouvy je možné měnit písemným oznámením doručeným druhé smluvní straně, s účinnosti ode dne doručení takového oznámení, a to bez nutnosti uzavírat dodatek ke Smlouvě.
7. Nebyla-li do okamžiku uplatnění záruky uhrazena celá kupní cena v souladu s touto Smlouvou, Kupující:
   a) není v prodlení s úhradou kupní ceny až do odstranění vady Předmětu koupě,
   b) není povinen uhradit kupní cenu ve výši odpovídající jeho nároku na slevu, jestliže vada Předmětu koupě je vyřešena poskytnutím slevy z kupní ceny.

VIII.
Smluvní sankce a odstoupení od Smlouvy

1. Smluvní strana není za prodlení se splněním svých závazků vyplývajících z této Smlouvy odpovědna, nemůže-li plnit v důsledku prodlení druhé smluvní strany.
2. Ujednává se smluvní pokuta pro případ, že Prodávající nedodrží termín dodání, implementace a předání Předmětu koupě sjednaný v této Smlouvě. Prodávající uhradí Kupujícímu smluvní pokutu ve výši 0,1 % z ceny dílčího plnění bez DPH za každý započatý den prodlení.
3. V případě prodlení Prodávajícího se zahájením odstraňování vady Předmětu koupě podle čl. VII. odst. 4 Smlouvy, je Kupující oprávněn požadovat smluvní pokutu ve výši 0,1% z celkové kupní ceny, a to za každý i započatý den tohoto prodlení.
4. Ujednává se smluvní pokuta za prokázané závažné nesplnění povinností Prodávajícího v souladu s relevantními právními předpisy, technickými normami, specifikací Předmětu koupě schválenou Kupujícím či jinými povinnostmi danými touto Smlouvou, a to ve výši 2 % z celkové ceny uvedené v čl. V. této Smlouvy za každý jednotlivý případ porušení povinnosti.
5. Ujednává se smluvní úrok z prodlení pro případ prodlení Kupujícího s úhradou faktury v dohodnutém termínu. Kupující má právo požadovat po Prodávajícím úrok z prodlení ve výši 0,01 % z dlužné částky

za každý započatý den prodlení.

6. Celková výše smluvních pokut je omezena limitem 100 % výše ceny uvedené v čl. V. Smlouvy a smluvní pokuty mohou být kombinovány (tzn., že uplatnění jedné smluvní pokuty nevylučuje souběžné uplatnění jakékoliv jiné smluvní pokuty).
7. Uplatnění kterékoliv ze smluvních pokut nezbavuje Kupujícího práva k uplatnění případné náhrady vzniklé škody, přičemž se částka zaplacených smluvních pokut do výše náhrady škody nezapočítává.
8. Veškeré smluvní sankce jsou splatné do 30 dnů po doručení oznámení o uložení smluvní pokuty druhé straně. Oznámení o uložení smluvní sankce musí vždy obsahovat popis a časové určení události, která v souladu s uzavřenou Smlouvou zakládá právo smluvní strany účtovat smluvní sankci. Oznámení musí dále obsahovat informaci o způsobu úhrady smluvní sankce. Kupující si vyhrazuje právo na určení způsobu úhrady smluvní pokuty, a to včetně formou zápočtu proti kterékoliv splatné pohledávce Prodávajícího vůči Kupujícímu.
9. Nedotčena zůstávají práva Kupujícího i Prodávajícího na náhradu škody a ušlý zisk nad rámec smluvní pokuty podle příslušných ustanovení Občanského zákoníku. Ohledně odpovědnosti z vad a odpovědnosti za škodu se smluvní strany řídí ustanoveními § 2099 a násl. Občanského zákoníku.
10. Obě smluvní strany jsou oprávněny s okamžitou platností odstoupit od této Smlouvy v případě podstatného porušení povinností druhou smluvní stranou. V tom případě je smluvní strana odstupující od Smlouvy povinna oznámit odstoupení od Smlouvy druhé smluvní straně bez zbytečného odkladu poté, co se o jejím podstatném porušení smluvních povinností dozvěděla. Za podstatné porušení smluvních povinností se rozumí zejména:
    a) prodlení Prodávajícího se splněním závazku odevzdat Předmět koupě Kupujícímu po dobu delší než 30 (slovy: třicet) kalendářních dnů;
    b) jestliže bylo vůči Prodávajícímu zahájeno řízení podle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů;
    c) prodlení Kupujícího se zaplacením kupní ceny o více než 30 (slovy: třicet) kalendářních dnů,
    d) případ, když Prodávající uvedl v nabídce do výběrového řízení informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek výběrového řízení.
    e) pokud dodaný Předmět koupě nesplňuje veškeré vlastnosti (parametry) stanovené touto Smlouvou. Prodávající v takovém případě nemá nárok na náhradu škody ani na náhradu účelně vynaložených nákladů.
11. Zakládá-li prodlení jedné ze smluvních stran nepodstatné porušení její smluvní povinnosti, může druhá strana od Smlouvy odstoupit poté, co smluvní strana v prodlení svoji povinnost nesplní ani v dodatečné přiměřené lhůtě, kterou jí druhá smluvní strana poskytla výslovně nebo mlčky. Oznámí-li oprávněná smluvní strana povinné smluvní straně, že ji určuje dodatečnou lhůtu k plnění a že jí již neprodlouží, platí, že marným uplynutím této lhůty oprávněná smluvní strana od Smlouvy odstoupila.
12. Odstoupením od Smlouvy se závazky z této Smlouvy zrušují s účinky ex nunc. Odstoupením od Smlouvy zanikají v rozsahu jeho účinků práva a povinnosti smluvních stran. Odstoupení od Smlouvy se nedotýká práva na zaplacení smluvní pokuty nebo úroku z prodlení, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany i po odstoupení od Smlouvy. Byl-li dluh zajištěn, nedotýká se odstoupení od Smlouvy ani zajištění.

IX.
Práva duševního vlastnictví

1. Prodávající odpovídá Kupujícímu za to, že má ve svém držení veškerá práva potřebná pro plnění svých povinností podle této smlouvy, a že vlastní veškeré vynálezy, znalosti, patenty, know-how a softwarové prostředky či jakákoliv jiná práva nutná ke splnění jeho závazků.
2. Prodávající uděluje Kupujícímu nevýhradní, teritoriálně neomezenou, převoditelnou a časově neomezenou licenci k SW, specifikovanému v Příloze č. 1 této smlouvy, v rámci autorských práv, patentu nebo jiných práv na průmyslová vlastnictví vlastněných Prodávajícím nebo třetí stranou, od které obdržel právo udělovat licenci a rovněž se zavazuje udělit Kupujícímu nevýhradní, teritoriálně omezené územím České republiky, převoditelné a časově neomezené právo používat know-how a

jiné technické informace předané Kupujícímu v rámci plnění této smlouvy. Prodávající se zavazuje u svých zaměstnanců a subdodavatelů zajistit, že Kupující bude oprávněn užívat, provozovat, opravovat, udržovat dílo a HW a jakoukoliv jejich část bez jejich souhlasu a bez toho, aby byl povinen platit těmto osobám zvláštní odměnu.

3. Pokud se ukáže, že licence, dodané Kupujícímu Prodávajícím v rámci plnění této smlouvy, nepokrývají veškeré licencované činnosti, nutné k užívání technologií, zavazuje se Prodávající na vlastní náklady zajistit pro Kupujícího chybějící časově neomezené nevýhradní licence, a to do pěti (5) dnů ode dne, kdy dojde ke zjištění chybějící licence. Toto ustanovení se netýká licencí, které má pod svou správou Kupující (serverové a databázové licence, licence operačních systémů).

X.

Vyšší moc, prodlení smluvních stran

1. Pokud některé ze smluvních stran brání ve splnění jakékoli její povinnosti z této smlouvy překážka v podobě vyšší moci, nebude tato smluvní strana v prodlení se splněním příslušné povinnosti, ani odpovědná za újmu plynoucí z jejího porušení. Pro vyloučení pochybností se předchozí věta uplatní pouze ve vztahu k povinnosti, jejíž splnění je přímo nebo bezprostředně vyloučeno vyšší mocí.

2. Vyšší mocí se pro účely této smlouvy rozumí mimořádná událost, okolnost nebo překážka, kterou příslušná smluvní strana při vynaložení náležité péče nemohla před uzavřením této smlouvy předvídat ani jí předejít a která je mimo jakoukoliv kontrolu takové smluvní strany a nebyla způsobena úmyslně ani z nedbalosti jednáním nebo opomenutím této smluvní strany. Takovými událostmi, okolnostmi nebo překážkami jsou zejména, nikoliv však výlučně:

   (i.) živelné události – zemětřesení, záplavy, vichřice atd.;

   (ii.) události související s činností člověka – např. války, občanské nepokoje, havárie letadel, radioaktivní zamoření štěpným materiálem nebo radioaktivním odpadem, nikoli však stávky zaměstnanců, hospodářské poměry a podobné okolnosti související s činností Strany, která se Vyšší moci dovolává;

   (iii.) epidemie, karanténa, či krizová a další opatření orgánů veřejné moci, a to zejména epidemie koronaviru označovaného jako SARS CoV-2 (způsobujícího nemoc COVID-19, jak může být virus někdy také v praxi označován), a s tím související existující či budoucí krizová opatření, jiná opatření, nové právní předpisy, správní akty či zásahy orgánů veřejné moci České republiky či jiných států,

   (iv.) obecně závazné akty státních a místních orgánů – zákony, nařízení, vyhlášky atd., včetně pokynů Kupujícího z nich nezbytně vycházejících, nikoli však správní, soudní nebo jiná rozhodnutí v konkrétní věci vydaná k tíži smluvní strany dovolávající se zásahu vyšší moci, pokud je důvodem jejich vydání porušení právní povinnosti touto smluvní stranou nebo její nedbalost.

3. Pro vyloučení pochybností se uvádí, že za vyšší moc se nepovažuje jakékoliv prodlení s plněním závazků kteréhokoli z poddodavatelů Prodávajícího, jakož ani finanční situace, insolvence, reorganizace, konkurs, vyrovnání, likvidace či jiná obdobná událost týkající se Prodávajícího nebo jakéhokoliv jeho poddodavatele nebo exekuce na majetek prodávajícího nebo jakéhokoliv smluvního dodavatele Prodávajícího.

4. Smluvní strana dotčená vyšší mocí je povinna informovat druhou smluvní stranu o existenci překážky v podobě vyšší moci bez zbytečného odkladu a dále podniknout veškeré kroky, které lze po takové smluvní straně rozumně požadovat, aby se zmírnil vliv vyšší moci na plnění povinností dle smlouvy.

5. Pokud bude zásah vyšší moci přetrvávat déle než [6 (slovy šest) měsíců], je kterákoliv ze smluvních stran oprávněna od této smlouvy odstoupit. Na základě odstoupení od této smlouvy z tohoto důvodu nevznikají

druhé smluvní straně žádné nároky na náhradu škody nebo smluvní pokuty, jež jinak tato smlouva může s odstoupením spojovat, nejsou však dotčeny nároky smluvních stran řádně vzniklé do té doby.

6. Žádná smluvní strana není odpovědná za prodlení se splněním svého závazku v případě, že i druhá smluvní strana je v prodlení se splněním svého synallagmatického závazku.

XI.
Závěrečná ujednání

1. Práva a povinnosti, které nejsou upraveny touto Smlouvou, se řídí příslušnými ustanoveními Občanského zákoníku a ostatními právními předpisy.
2. V případě, že se ke kterémukoli ustanovení této Smlouvy či k jeho části podle Občanského zákoníku jako ke zdánlivému právnímu jednání nepřihlíží, nebo že kterékoli ustanovení této Smlouvy či jeho část je nebo se stane neplatným, neúčinným anebo nevymahatelným, oddělí se v příslušném rozsahu od ostatních ujednání této Smlouvy a nebude mít žádný vliv na platnost, účinnost a vymahatelnost ostatních ujednání této Smlouvy. Smluvní strany se zavazují nahradit takové zdánlivé, nebo neplatné, neúčinné a nebo nevymahatelné ustanovení či jeho část ustanovením novým, které bude platné, účinné a vymahatelné a jehož věcný obsah a ekonomický význam bude shodný nebo co nejvíce podobný nahrazovanému ustanovení tak, aby účel a smysl této smlouvy zůstal zachován.
3. Dle § 1765 Občanského zákoníku na sebe Prodávající převzal nebezpečí změny okolností. Před uzavřením Smlouvy smluvní strany zvážily hospodářskou, ekonomickou i faktickou situaci a jsou si plně vědomy okolností Smlouvy. Prodávající není oprávněn domáhat se změny Smlouvy v tomto smyslu u soudu.
4. Smluvní strany výslovně souhlasí s tím, aby tato Smlouva byla uvedena v Centrální evidenci smluv Technické správy komunikací hl. m. Prahy, a.s. (CES TSK) vedené Kupujícím, která je veřejně přístupná a která obsahuje údaje o smluvních stranách, předmětu Smlouvy, číselné označení této Smlouvy a datum jejího podpisu.
5. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu § 504 občanského zákoníku a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoli dalších podmínek.
6. Smluvní strany výslovně sjednávají, že uveřejnění této smlouvy v registru smluv dle zákona č.340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění, zajistí Kupující.
7. Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti uveřejněním v registru smluv dle zákona o registru smluv.
8. Každá ze smluvních stran potvrzuje, že při sjednávání této Smlouvy postupovala čestně a transparentně a současně se zavazuje, že takto bude postupovat i při plnění této Smlouvy a veškerých činnostech s ní souvisejících. Smluvní strany potvrzují, že se seznámily se zásadami Criminal compliance programu Technické správy komunikací hl. m. Prahy, a.s. (dále jen „CCP"), které jsou zveřejněny na webových stránkách Kupujícího, zejména s Kodexem CCP a zavazují se tyto zásady po dobu trvání smluvního vztahu dodržovat. Každá ze smluvních stran se zavazuje, že bude jednat a přijme opatření tak, aby nevzniklo důvodné podezření na spáchání trestného činu či k jeho spáchání, tj. tak, aby kterékoli ze smluvních stran nemohla být přičtena odpovědnost podle zák. č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, nebo nevznikla trestní odpovědnost jednajících osob podle zák. č. 40/2009 Sb., trestní zákoník.
9. Obě smluvní strany současně prohlašují, že všechna ustanovení této Smlouvy byla prohlášena za podstatná. Smlouva je vyhotovena v 5 stejnopisech, z nichž 2 stejnopisy obdrží Prodávající a tři Kupující. V případě, že je Smlouva uzavírána elektronicky za využití kvalifikovaných elektronických

podpisů, postačí jedno vyhotovení Smlouvy, na kterém jsou zaznamenány kvalifikované elektronické podpisy zástupců Stran v souladu s příslušnými ustanoveními zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

10. Dále smluvní strany prohlašují, že tato Smlouva nebyla sepsána za nápadně nevýhodných podmínek. Obě smluvní strany si ponechávají právo na možnost odstoupení od Smlouvy, a to v tom případě, když jedna ze smluvních stran nebude moci z vážných důvodů splnit svůj závazek ve smyslu předchozích ustanovení a dále si smluvní strany ponechávají právo na náhrady škody.
11. Každá ze smluvních stran prohlašuje, že tuto Smlouvu uzavírá svobodně a vážně, že považuje obsah této Smlouvy za určitý a srozumitelný a že jsou jí známy všechny skutečnosti, jež jsou pro uzavření této Smlouvy rozhodující.
12. Změny a doplňky v této Smlouvě se činí písemně, a to formou dodatku ke Smlouvě.
13. Nedílnou součástí této Smlouvy je:
    a) Příloha č. 1 - Technická specifikace
    b) Příloha č. 2 - Minimální seznam podporovaných zdrojů logů
    c) Příloha č. 3 - Podrobná specifikace ceny

V Praze dne .....

Za Kupujícího:
Technická správa komunikací hl. m. Prahy a.s.

[redacted]
Datum: 2020.12.07 10:57:39 +01'00'

.....
Michal Berounský
ředitel úseku informatiky,
na základě pověření

V Praze dne .....

Za Prodávajícího:
COMTESYS, spol. s r.o.

[redacted]
VOBOŘIL Datum: 2020.12.04 14:47:10 +01'00'

.....
Ing. Martin Vobořil
jednatel společnosti

Příloha č. 1 – technická specifikace

Technická specifikace

Systém umožní procházení logů integrovaným grafickým rozhraním s předdefinovanými pravidly pro rychlé vyhledávání (např. jako jsou změny v systémech provedené administrátory; seznam nově vytvořených účtů v MS Active Directory za zvolenou periodu; změny v přístupových právech pro zadaného uživatele nebo k zadané složce; monitoring privilegovaných účtů, sdílených účtů a změn konfigurací; sledování souborových systémů apod.) Dále musí systém umožňovat sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

Implementací systému dojde k zavedení jednotného úložiště logů s pokročilými nástroji analýzy a upozorňování ke kterému budou mít přístup pouze autorizovaní pracovníci Kupujícího. Systém umožní vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Systém musí dále umožňovat tvorbu uživatelsky definovaných parserů, upozornění a korelací bez potřeby účasti výrobce nebo dodavatele. Součástí dokumentace k systému bude jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů. Systém umožní zálohování konfigurace i dat a jejich obnovu.

Dodaný systém musí podporovat plánované zálohování i zálohování ad-hoc vzniklých dat na externí zálohovací systém za využití SMB protokolu. Zálohováním dat na externí systém musí umožnit dosažení požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců – dle "Bezpečnostního doporučení NCKB pro Administrátory 2.0". Systém musí dále umožňovat on-line zobrazení hodnot nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat.

Číslo	Popis - Řešení SEM/SIEM do 5000 událostí/s s minimálně 40TB velikostí databáze
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat
1	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware
3	Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli není povinná konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se skripty/makra vkládají.
4	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. poddodavatelů) 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. Součást dodávky tvoří příslušná dokumentace k vytváření parserů a testování jejich funkčnosti.

5	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Bude předložen příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.
6	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále musí systém umožnit podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL. Součást dodávky tvoří detailní komunikační matrice nabízeného systému a dokumentace k nastavení ODBC v grafickém rozhraní systému.
7	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, při minimálním 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.
8	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
9	Standardizované pole dekódované z přijatých zpráv musí provádět minimálně tyto operace (pokud zdrojový log tyto informace obsahuje), názvy polí se můžou lišit, nicméně musí být v dodaném systému konzistentní - username = uživatelské jméno (malým písmem), src_ip = zdrojová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, dst_ip = cílová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, src_port = zdrojový port uložený v číselné podobě, dst_port = cílový port uložený v číselné podobě, protocol = druh přenosového protokolu, status = informace o stavu provedené akce (úspěch/neúspěch apod.), duration = kolik vteřin událost trvala uložena v číselné podobě.
10	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí.
11	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
12	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
13	Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
14	Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Součástí dodávky je i odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.
15	Systém provádí konsolidaci logů na interním storage logovacího systému.
16	Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Součást dokumentace k systému tvoří link nebo pdf popisující způsob vytváření reportů.

17	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
18	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
19	Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.
20	Systém podporuje nativní získávání logů z Office365. Součástí dodávky je link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.
21	V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.
22	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
23	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 a nelze je nahradit čestným prohlášením.
24	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem systému nevratně modifikovat.
25	Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
26	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
27	Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
28	Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Součástí dodávky je link na online dokumentaci nebo připojení pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.
29	Systém nabízí kapacitní i výkonovou škálovatelnost.
30	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.
31	Ze systému musí být možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.
32	Systém umožní monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.
33	Systém musí obsahovat REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Součástí dodávky je předložení vzorového návodu na integraci s externím monitorovacím systémem.

34	Součástí dodávky je prohlášení výrobce o shodě v souladu s požadavky Vyhlášky č. 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 č. 181/2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)".
35	Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním. Součástí dodávky je dokumentace, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.
36	Systém musí umožňovat jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. Součástí dodávky je odkaz na dokumentaci popisující vytváření uživatelských rolí.
37	Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.
38	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
	Minimální HW parametry požadovaného systému
39	Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
40	HW appliance obsahující veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.
41	2 procesory, min. 12 jader každý, s podporou HyperThreadingu.
42	Min. 128GB DDR-4 a NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).
43	Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 8GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.
44	V systému musí být minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.
45	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad) ve webovém rozhraní systému a příslušný popis v dokumentaci.
46	Větráky v systému musí být vyměnitelné za provozu a redundantní.
47	2x napájecí zdroje s redundancí napájení 1+1.
48	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
49	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).
	Výkonnostní a SW parametry systému
50	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli, například není nutné editovat žádné konfigurační soubory, scripty nebo makra).
51	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Součástí dodávky je předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.

52	Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Součástí dodané dokumentace musí být podrobný způsob realizace downgrade.
53	Průměrný trvalý příjem min. 6 tisíc událostí/s. Výkon musí odpovídat pro požadované množství událostí s průměrnou délkou 600Byte.
54	Špičkový příjem minimálně 12 tisíc událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí, než je průměrný trvalý příjem, je systém uloží do bufferu a zpracuje později.
55	Systém umožní licenčně neomezený počet zařízení pro příjem zasílaných událostí, tj. licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40TB a nad to musí podporovat kompresi ukládaných dat.
56	Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi.
57	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.
58	Systém musí podporovat doplňování zpráv o statické informace z textových tabulek. (Například k uživatelskému jménu doplnit informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes webové rozhraní.
59	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů musí být možnost vložení minimálně 20 testovacích zpráv současně. Součástí dodávané dokumentace je odkaz, ze kterého je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.
60	V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...
61	V centrální správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).
62	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.
63	Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – požadujeme podporu minimálně 2 nodů. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.

64	Dvounodový cluster se chová jako 1 celek. V případě využití dvou nodů v clusteru se zrychluje vyhledávání a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.
65	V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu (řízenou aktivním prvkem počítačové sítě) a zároveň cluster musí zajišťovat synchronizaci konfigurace a událostí mezi nody.
66	Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.
67	Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
68	Systém umožňuje podporu zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.
69	Součástí systému je podpora zálohování dat na externí systém. Je požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Systém umožňuje obnovit data ze záloh a během obnovy je automaticky znova indexovat tak, aby bylo možné v datech obnovených ze záloh pracovat shodně jako s aktuálním obsahem databáze. Zálohování musí jít kompletně nastavit v uživatelském rozhraní systému, nepřipouští se využívání scriptů, maker nebo textových konfiguračních souborů. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.
	Alerty
70	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
71	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
72	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.
73	Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Součástí dodávky je odkaz na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.
74	Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu je vyžadována možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.
75	V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality).
76	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci.
	Sběr událostí z Microsoft prostředí
77	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Součástí dodávky je předložení kompletní dokumentace a poznámek k vydání (release notes) k agentu pro sběr událostí z prostředí Microsoft.
78	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.
79	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.

80	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.
81	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se centrálně z grafického rozhraní spravují Windows agenti včetně všech možností nastavení.
82	Agent automaticky překládá zástupné kódy status ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).
83	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.
84	Komunikace Windows agenta a centrálního systému musí být šifrovaná.
85	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.
86	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.
87	Počet instalací Windows agenta nesmí být licenčně a časově omezen.
	Podpora pro sběr událostí z poboček
88	Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Součástí dodávky je odkaz na dokumentaci, jakým způsobem se realizuje sběr událostí z poboček.
89	Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
90	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.
91	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.
92	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
93	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.
94	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
95	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
96	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
	Vysoká dostupnost, SW Podpora a záruka na hardware

97	Naplnění požadavku volitelné podpory pro nasazení ve vysoké dostupnosti.
98	HW - 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.
99	SW - Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem

Příloha č. 2 - Minimální seznam podporovaných zdrojů logů

Seznam povinně podporovaných zdrojů logů
Apache httpd
Apache Tomcat
Amavis
Antivir Eset
Antivir Eset Remote administrator
Brocade FC switches
ArcSight CEF format all sources
Cisco ASA
Cisco Firepower
Cisco IOS
Cisco IronPort
Cisco Nexus
Cisco SMB
Cisco WLC
Dell Force10
Dell iDrac (Server OoB management)
Dell PowerConnect
Dell SonicWALL
Discard (Special distard rule)
Dropbear SSH (mostly Embedded Linux)
FlowMon
FortiAuthenticator
FortiDDoS
Fortigate
FortiGate-Lite (performance optimized)
FortiMail
FortiManager
FreeRADIUS
Qradar LEEF format all sources
HAProxy (structured rfc5425 logformat)
HPE Aruba Instant AP (WLAN)
HPE Aruba Mobility Controller (WLAN)
HPE iLo 4 (Server OoB management)
HPE IMC
HPE routers
HPE switches Procurve OS
HPE switches Comware OS
HPE Comware WLAN
CheckPoint LOG Exporter
CheckPoint via OPSEC protocol
ISC BIND

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

Příloha č. 3 - Podrobná specifikace ceny

Systém pro centralizovanou správu logů, událostí a strojových dat

Dodávka HW appliance LOGmanager-L (5 let HW záruka, 5 let SW renewal, 1x LOGmanager-VF, 40 TB databáze)

LOGmanager je HW řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s obrovskou kapacitou, rychlým vyhledáváním ve "velkých datech" a okamžitou vizualizací vyžádaných dat.

LOGmanager nativně podporuje více než 125 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes sítě, virtualizace, operační systémy, databáze, až po cloud aplikace. Seznam zdrojů se každou aktualizací rozšiřuje. LOGmanager dále podporuje standardizované strukturované formáty logů jako jsou CEF, LEEF, RFC5424 a JSON. Pro unikátní zdroje dat umožňuje rychlé a snadné vytvoření zákaznických parserů.

Klíčové vlastnosti

- Centrální úložiště logů, událostí a strojových dat organizace
- Sjednocení formátu zdrojových logů do uživatelsky srozumitelné formy
- Zpracování a vizualizace přijímaných dat v reálném čase
- Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- SIEM funkce. Alerty na základě podmínek s limity a korelacemi
- Unikátní grafické konfigurační a programovací rozhraní
- Radikální jednoduchost a uživatelská přívětivost
- Snadné vytváření reportů a auditních zpráv za běhu
- Umožnění snadnějších splnění požadavku na shodu s regulacemi pro:
    - GDPR
    - Zákon o kybernetické bezpečnosti a návazné vyhlášky
    - ČSN/ISO 27001:2013 pro pořizování auditních záznamů
    - PCI DSS 3.2
- Bez licenčních omezení na množství zdrojů, výkon a uložená data
- Úspora na licencích při budoucím rozšíření směrem k SIEM/UBA

Implementace:

- Fyzická instalace, zapojení logmanageru do sítě a nastavení logování:
- síťových prvků (včetně poboček)
- bezdrátových síťových prvků
- bezpečnostních prvků (Check Point)
- operačních systémů na serverech (Windows, Linux)
- virtualizačního prostředí (VMware)
- koncová konzultace s ohledem na email alertování kritických událostí případně týdenních reportů

Cena:

Popis	MJ	Cena MJ	Celkem
LOGmanager-L (5 let HW záruka, 5 let SW renewal, 1x LOGmanager-VF, 40 TB databáze)	[redacted]		
Implementace do prostředí TSK			
Celkem bez DPH			**1 190 400 Kč**
Výše DPH 21 %			**249 984 Kč**
Celkem s DPH			**1 440 384 Kč**