Kupní smlouva

I. Smluvní strany

Masarykův onkologický ústav
se sídlem Žlutý kopec 7, 656 53 Brno
zastoupený prof. MUDr. Janem Žaloudíkem, CSc., ředitelem
IČO: 00209805, DIČ: CZ00209805
bankovní spojení: Česká národní banka, č. ú.: 87535621/0710
(dále jen *„kupující“*)

a

DATASYS s.r.o.
se sídlem Jeseniova 2829/20, 130 00 Praha 3
zastoupený Ing. Markem Růžičkou, Ph.D., prokuristou
IČO: 61249157 DIČ: CZ61249157
bankovní spojení: Komerční banka, a.s. č. ú.: 27-9647490267/0100
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze oddíl C, vložka 28862
(dále jen *„prodávající“*)

na základě zadávacího řízení k veřejné zakázce *„Centrální úložiště logů“* zadávané podle zákona č. 134/2016. Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a v souladu s Obecnými pravidly pro žadatele a příjemce Integrovaného regionálního operačního programu (vydání 1.11, platnými od 15. 5. 2018) v rámci projektu: *„Zvýšení kybernetické bezpečnosti v Masarykově onkologickém ústavu“*, registrační číslo projektu: *CZ.06.3.05/0.0/0.0/15_011/0006934* (dále jen *„projekt“*) kupujícím, uzavírají v souladu s § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen *„občanský zákoník“*), tuto smlouvu (dále jen *„smlouva“*):

II. Předmět smlouvy

(1) Prodávající se smlouvou zavazuje dodat kupujícímu centrální úložiště logů dle specifikace uvedené v příloze č. 1 smlouvy (dále jen *„centrální úložiště logů“*).

(2) Prodávající se smlouvou zároveň zavazuje k:
- instalaci a implementaci centrálního úložiště logů,
- zajištění licenčních oprávnění k softwarové části centrálního úložiště logů,
- dodání technické dokumentace a návodů k centrálnímu úložišti logů v českém nebo anglickém jazyce,
- dodání dokladů osvědčujících způsobilost hardwarové části centrálního úložiště logů k účelu užívání v České republice,
- dodání dokladů nutných k převzetí a řádnému užívání hardwarové části centrálního úložiště logů, zejména prohlášení o shodě dle zákona č. 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů,
- provedení školení pro 5 pracovníků kupujícího,
- poskytnutí dalších služeb vymezených ve smlouvě.

(3) Kupující se smlouvou zavazuje řádně a včas dodané centrální úložiště logů převzít a zaplatit za něj dohodnutou cenu a dále se zavazuje platit za řádně a včas poskytované další služby vymezené ve smlouvě.

III. Kupní cena a platební podmínky

(1) Cena za splnění závazků prodávajícího vyplývajících ze smlouvy s výjimkou ceny servisní podpory (dále jen *„kupní cena“*) činí:

Kupní cena bez DPH:	1 099 160,00 Kč
DPH (21) %:	230 823,60 Kč
Kupní cena včetně DPH:	**1 329 983,60 Kč**

(2) Cena servisní podpory činí:

Cena servisní podpory bez DPH:	179 860,00 Kč / 1 rok
DPH (21) %:	37 770,60 Kč / 1 rok
Cena servisní podpory včetně DPH:	**217 630,60 Kč / 1 rok**

(3) Rozklad kupní ceny a ceny servisní podpory je uveden v příloze č. 2 smlouvy.

(4) Kupní cena a cena servisní podpory je stanovena jako konečná, pevná a nepřekročitelná. Kupní cena a cena servisní podpory může být změněna pouze v případě změny sazby daně z přidané hodnoty. V takovém případě se složka ceny, kterou tvoří daň z přidané hodnoty, upraví v souladu s právními předpisy.

(5) Kupní cena (resp. cena servisní podpory) zahrnuje veškeré náklady související se splněním závazků prodávajícího ze smlouvy, včetně odvozu a likvidace obalů a dalších materiálů, veškerých organizačních a koordinačních činností, manipulace s hardwarovou částí centrálního úložiště logů, licenčních oprávnění k softwarové části centrálního úložiště logů apod.

(6) Kupní cena bude uhrazena po protokolárním předání a převzetí centrálního úložiště logů, a to na základě daňového dokladu (faktury) vystaveného prodávajícím po předání a převzetí centrálního úložiště logů kupujícím se splatností do 30 dnů ode dne doručení daňového dokladu kupujícímu. Cena servisní podpory bude hrazena vždy na 1 rok předem, a to na základě daňového dokladu (faktury) vystaveného prodávajícím na první rok po předání a převzetí centrálního úložiště logů kupujícím se splatností do 30 dnů ode dne doručení daňového dokladu kupujícímu, následně vždy nejdříve 1 kalendářní měsíc před koncem předchozího ročního období.

(7) Daňový doklad musí být v souladu s platnými právními předpisy, zejména se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. V případě, že daňový doklad nebude obsahovat náležitosti dle platných právních předpisů, popř. bude obsahovat jiné chyby či nedostatky, je kupující oprávněn takový daňový doklad vrátit, přičemž nová doba splatnosti počíná běžet dnem doručení opraveného daňového dokladu kupujícímu.

(8) Na daňovém dokladu bude uveden název veřejné zakázky: *„Centrální úložiště logů“* a číslo projektu: CZ.06.3.05/0.0/0.0/15_011/0006934.

(9) Bude-li k datu uskutečnění zdanitelného plnění nebo k datu poskytnutí úplaty za takové plnění prodávající nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen *„ZoDPH“*), nebo bude-li na daňovém dokladu uveden bankovní účet nezveřejněný v souladu s § 109 odst. 2 písm. c) ZoDPH, je kupující oprávněn postupovat dle § 109a ZoDPH, tj. uhradit část kupní ceny odpovídající výši vypočtené daně z přidané hodnoty přímo na bankovní účet příslušného správce daně (jako úhradu daně za poskytovatele zdanitelného plnění z takového zdanitelného plnění), přičemž se tímto považuje daná část ceny za uhrazenou.

IV. Doba a místo dodání

(1) Prodávající se zavazuje dodat centrální úložiště logů a provést jeho implementaci v rozsahu uvedeném ve smlouvě do 70 kalendářních dnů ode dne nabytí účinnosti smlouvy.

(2) Hardware a software budou dodány do prostor Masarykova onkologického ústavu, Žlutý kopec 7, 656 53 Brno (Úsek informačních technologií, Švejdův pavilon).

V. Předání a převzetí centrálního úložiště logů

(1) Prodávající se zavazuje nahlásit termín dodávky a implementace centrálního úložiště logů minimálně tři dny předem, a to [redacted], vedoucímu Úseku informačních technologií, tel.: [redacted], e-mail: [redacted], a [redacted], vedoucímu Obchodního oddělení, tel.: [redacted], e-mail: [redacted].

(2) Kupující je oprávněn přizvat k předání a převzetí centrálního úložiště logů i jiné osoby.

(3) O průběhu předávacího a přejímacího řízení pořídí prodávající zápis (protokol), jehož povinnými údaji jsou:

- údaje o smluvních stranách,
- popis centrálního úložiště logů,
- sériová čísla dodávané hardwarové části centrálního úložiště logů,
- doklady prokazující sjednání odstraňování vad hardwarové části centrálního úložiště logů ze strany jeho výrobce,
- doklady prokazující sjednání služeb výrobce softwarové části centrálního úložiště logů dle čl. VII. odst. (3) smlouvy,

- případné výhrady kupujícího k centrálnímu úložišti logů,
- prohlášení kupujícího, zda centrální úložiště logů převzal nebo nepřevzal,
- případné odůvodnění, proč kupující centrální úložiště logů nepřevzal,
- soupis předávaných dokladů vztahujících se k centrálnímu úložišti logů.

(4) Kupující je povinen převzít řádně a včas dodané a implementované centrální úložiště logů, tj. které vykazuje všechny vlastnosti a vyhovuje všem podmínkám uvedeným ve smlouvě či stanoveným kupujícím nebo právními předpisy a technickými normami a u kterého bylo provedeno školení.

(5) Kupující není povinen převzít centrální úložiště logů zejména v následujících případech:
- hardwarová část centrálního úložiště logů vykazuje známky poškození,
- k softwarové části centrálního úložiště logů nejsou zajištěna potřebná licenční oprávnění,
- centrální úložiště logů vykazuje vady, které brání jeho řádnému užívání,
- není předána veškerá dokumentace k centrálnímu úložišti logů v souladu se smlouvou,
- centrální úložiště logů není dodáno a implementováno v termínu uvedeném ve smlouvě.

(6) Náklady na případný odvoz hardwarové části centrálního úložiště logů (včetně balného), které kupující v souladu se smlouvou nepřevzal, nese prodávající.

(7) Kupující je oprávněn převzít i takové centrální úložiště logů, které vykazuje vady, které nebrání jeho řádnému užívání. Tyto vady se vyznačí v protokolu při přejímacím řízení. Prodávající je povinen tyto vady bezodkladně, nejpozději však do 30 kalendářních dnů, odstranit.

(8) Centrální úložiště logů se považuje za předané a převzaté okamžikem podpisu předávacího protokolu kupujícím, ze kterého vyplývá, že kupující centrální úložiště logů přebírá.

VI. Nebezpečí škody, přechod vlastnického práva

(1) Okamžikem předání a převzetí centrálního úložiště logů kupujícím přechází na kupujícího nebezpečí škody na hardwarové části centrálního úložiště logů.

(2) Okamžikem předání a převzetí hardware kupujícím přechází na kupujícího vlastnické právo k hardwarové části centrálního úložiště logů.

VII. Odpovědnost za vady, záruka za jakost, servisní podpora

(1) Prodávající odpovídá za vady, jež má centrální úložiště logů v době jeho předání. Záruka za jakost se nesjednává.

(2) Prodávající se zavazuje zajistit kupujícímu odstraňování vad hardwarové části centrálního úložiště logů výrobcem této hardwarové části centrálního úložiště logů (dále také *„výrobce HW“*), a to po dobu 60 měsíců ode dne převzetí centrální úložiště logů. Výrobce HW musí být povinen odstraňovat vady hardwarové části centrální úložiště logů nejpozději nebližšího pracovního dne ode dne nahlášení vady. Cena za odstraňování vad je zahrnuta v kupní ceně.

(3) Prodávající se zavazuje zajistit kupujícímu takové služby výrobce softwarové části centrálního úložiště logů, které prodávajícímu umožní poskytovat kupujícímu níže uvedenou servisní podporu, a to po dobu 60 měsíců ode dne převzetí centrální úložiště logů.

(4) Prodávající se po dobu 60 měsíců ode dne převzetí centrálního úložiště logů zavazuje kupujícímu poskytovat následující služby (dále jen *„servisní podpora“*) spočívající v:
- přijímání hlášení o vadách centrálního úložiště logů prostřednictvím helpdeskového systému prodávajícího (např. prostřednictvím zákaznické zóny na jeho webových stránkách) na adrese https://helpdesk.datasys.cz či prostřednictvím e-mailové adresy [redacted], v pracovních dnech od 8.00 h do 17.00 h,
- odstranění vad softwarové části centrálního úložiště dat nejpozději:
  - v případě vady vylučující či významně omezující funkčnost centrálního úložiště logů – do 3 pracovních dnů ode dne, ve kterém je vada nahlášena,
  - v případě vady neomezující či nevýznamně omezující funkčnost centrálního úložiště logů – do 10 pracovních dnů ode dne, ve kterém je vada nahlášena,

  je-li vada nahlášena mimo období uvedené v prvním bodě tohoto odstavce, považuje se pro účely tohoto bodu za den nahlášení nejbližší pracovní den po dni, ve kterém skutečně

došlo k nahlášení vady, smluvní strany jsou oprávněny se v konkrétním případě domluvit na jiných lhůtách k odstranění vady,

- předávání požadavků na odstranění vady hardwarové části centrálního úložiště logů výrobci hardwarové části centrálního úložiště logů, a to nejpozději následujícího pracovního dne po dni, ve kterém je vada nahlášena (je-li vada nahlášena mimo období uvedené v prvním bodě, považuje se pro účely tohoto bodu za den nahlášení nejbližší pracovní den po dni, ve kterém skutečně došlo k nahlášení vady),
- podpůrných službách v rozsahu 40 hodin ročně spočívajících v údržbě centrálního úložiště logů (např. konfigurace sběru dat, vytváření dashbordů či vytváření „alertovacích" pravidel) a konzultačních službách týkajících se centrálního úložiště logů,
- provádění aktualizací softwarové části centrálního úložiště logů tak, aby byl zajištěn řádný provoz centrálního úložiště logů a bezpečnost v něm obsažených dat (stav, kdy neprovedením aktualizace softwarové části centrálního úložiště logů není zajištěn řádný provoz a bezpečnost centrálního úložiště logů se považuje za vadu softwarové části centrálního úložiště logů).

(5) Prodávající se při poskytování servisní podpory zavazuje komunikovat v českém jazyce.

(6) Prodávající se při poskytování servisní podpory zavazuje využívat přednostně vzdáleného přístupu, v této souvislosti se zavazuje uzavřít s kupujícím smlouvu o vzdáleném přístupu.

(7) Prodávající je oprávněn k plnění povinností vyplývajících z tohoto článku smlouvy využít poddodavatele.

VIII. Smluvní sankce

(1) V případě prodlení kupujícího s úhradou kupní ceny je kupující povinen uhradit prodávajícímu úrok z prodlení ve výši dle nařízení vlády č. 351/2013 Sb., ve znění pozdějších předpisů.

(2) V případě prodlení prodávajícího s dodáním centrálního úložiště logů v souladu se smlouvou je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 2.000 Kč, a to za každý započatý den prodlení.

(3) V případě prodlení prodávajícího s odstraněním vad vymezených v čl. V. odst. (7) smlouvy je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 1.000 Kč za každý započatý den prodlení.

(4) V případě prodlení prodávajícího s odstraněním vady softwarové části centrálního úložiště logů je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 2.000 Kč za každý započatý den prodlení.

(5) V případě prodlení prodávajícího s předáním požadavku na odstranění vady hardwarové části centrálního úložiště logů výrobci hardwarové části centrálního úložiště logů je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 2.000 Kč za každý započatý den prodlení.

(6) Prodávající je povinen uhradit smluvní pokutu kupujícímu do 10 dnů počítaných ode dne doručení jejího vyúčtování prodávajícímu.

(7) Zaplacení jakékoli z výše uvedených smluvních pokut se nedotýká nároku kupujícího na náhradu škody v plné výši.

IX. Platnost a účinnost smlouvy, změny smlouvy

(1) Smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti uveřejněním v Registru smluv (*smlouvy.gov.cz*).

(2) Plnění předmětu smlouvy před účinností smlouvy se považuje za plnění podle smlouvy a práva a povinnosti z něj vzniklé se řídí smlouvou.

(3) Veškeré změny smlouvy mohou být učiněny výhradně písemnou formou, prostřednictvím vzestupně číslovaných dodatků podepsaných oběma smluvními stranami.

(4) Pokud jakékoliv ustanovení smlouvy netvořící její podstatnou náležitost je nebo se stane neplatným nebo nevymahatelným jako celek nebo jeho část, je plně oddělitelným od ostatních ustanovení smlouvy a taková neplatnost nebo nevymahatelnost nebude mít žádný vliv na platnost a vymahatelnost jakýchkoliv ostatních ustanovení ze smlouvy, strany se zavazují v rámci smlouvy nahradit prostřednictvím dodatku k smlouvě toto neplatné nebo

nevymahatelné oddělené ustanovení takovým novým platným a vymahatelným ustanovením, jehož předmět bude v nejvyšší možné míře odpovídat předmětu původního odděleného ustanovení. Pokud však jakékoliv ustanovení smlouvy tvořící její podstatnou náležitost je nebo se stane neplatným nebo nevymahatelným jako celek nebo jeho část, strany nahradí neplatné nebo nevymahatelné ustanovení v rámci nové smlouvy takovým novým platným a vymahatelným ustanovením, jehož předmět bude v nejvyšší možné míře odpovídat předmětu původního ustanovení obsaženému ve smlouvě.

(5) Prodávající je oprávněn převést svoje práva a povinnosti ze smlouvy vyplývající na jinou osobu pouze s písemným souhlasem kupujícího.

(6) Kupující je oprávněn od smlouvy odstoupit zejména v případě:

- uvedeném v čl. VII. odst. 6) smlouvy,
- že je prodávající v prodlení s dodávkou a implementací centrálního úložiště logů déle než 30 dnů,
- že centrální úložiště logů nesplňuje požadavky uvedené ve smlouvě, požadavky právních předpisů, technických a jiných norem.

V ostatních případech je kupující oprávněn od smlouvy odstoupit v souladu s § 2001 občanského zákoníku.

(7) Prodávající je oprávněn od smlouvy odstoupit v případě, že kupující bude v prodlení s úhradou kupní ceny déle než 2 měsíce.

(8) Odstoupením od smlouvy se smlouva rozvazuje dnem doručení odstoupení druhé smluvní straně.

X. Ostatní ujednání

(1) Smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá smluvní strana obdrží po jednom.

(2) V otázkách výslovně neupravených smlouvou se závazky smluvních stran řídí ustanoveními příslušných právních předpisů, zejména § 2079 a násl. občanského zákoníku upravujícími kupní smlouvu.

(3) Osobou oprávněnou za kupujícího:

- k převzetí centrálního úložiště logů a podpisu předávacího protokolu,
- k reklamaci vad centrálního úložiště logů a podpisu servisních výkazů,

je [redacted], tel.: [redacted], e-mail: [redacted],

- ke komunikaci s oprávněnými zaměstnanci prodávajícího ohledně dodávky centrálního úložiště logů a souvisejících činností,

je [redacted], vedoucí Obchodního oddělení, tel.: [redacted], e-mail: [redacted].

(4) Smluvní strany souhlasí se zveřejněním smlouvy v úplném znění, stejně jako s uveřejněním úplného znění případných dohod (dodatků), kterými se smlouva doplňuje, mění, nahrazuje nebo ruší, a to zejména prostřednictvím Registru smluv (*smlouvy.gov.cz*) v souladu se zákonem č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Smluvní strany se dohodly, že uveřejnění smlouvy zajistí kupující.

(5) Prodávající si je vědom toho, že v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů, je osobou povinnou spolupůsobit při výkonu finanční kontroly. Prodávající se zavazuje poskytnout kontrolním orgánům při provádění kontroly maximální součinnost. Prodávající je zároveň povinen zavázat své subdodavatele, aby tito spolupůsobili při provádění kontroly a poskytovali kontrolním orgánům při provádění kontroly maximální součinnost.

(6) Prodávající si je vědom toho, že je povinen minimálně do konce roku 2028 uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů a poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a že je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

(7) Smluvní strany se v souladu s § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, dohodly, že místně příslušným soudem je Městský soud v Brně.

(8) Nedílnou součástí smlouvy jsou následující přílohy:
- Příloha č. 1 – *Technická specifikace centrálního úložiště logů*,
- Příloha č. 2 – *Rozklad kupní ceny.*

(9) Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že s jejím obsahem souhlasí a na důkaz výše uvedeného připojují své vlastnoruční podpisy.

V Brně dne 13. 06. 2019

[redacted]

_____

za kupujícího
prof. MUDr. Jan Žaloudík, CSc.
ředitel Masarykova onkologického ústavu

[redacted]

V Praze dne -5 -06- 2019

[redacted]

_____

za prodávajícího
Ing. Marek Růžička, Ph.D.
prokurista DATASYS s.r.o.

[redacted]

Příloha č. 1

Technická specifikace centrálního úložiště logů

Vlastnosti nástroje ELISA

DATASYS ELISA je robustní a výkonné řešení typu SIEM pro sběr, korelace a analýzu logů. Jádrem systému je extrémně rychlá „noSQL“ analytická databáze ***Elasticsearch*** s vylepšeným uživatelským rozhraním ***Kibana***, které poskytuje vysoký komfort při analýze detekovaných bezpečnostních incidentů a relevantních logů. Elasticsearch databázi je možné distribuovat na více serverů za účelem rozdělení zátěže a vysoké dostupnosti indexovaných dat.

Uživatelským prostředím je webový prohlížeč. Vyhledávání v databázi událostí je podobné s vyhledáváním v internetovém vyhledávači – prováděno jednoduše zadáním klíčových slov. Po krátkém zaškolení dokáže ale i nezkušený uživatel formulovat též komplexní filtry, které široce přesahují možnosti vyhledávání v relačních databázích. Definice filtrů lze ukládat pro opakované použití.

ELISA poskytuje díky své architektuře bleskové odezvy i v případě objemných indexů/databází. Uživateli je v základu zobrazen histogram počtu výskytů vyhovujících záznamů za zvolený časový interval a jejich tabulkový stránkovaný přehled. V odladěné konfiguraci našeho řešení ***ELISA*** jsou události přenášeny do analytické databáze v původní, strukturu záznamu zachovávající podobě, s bezproblémovou podporou diakritiky.

Označením konkrétní události získá uživatel přehled o všech jejích atributech a možnost drill-down analýzy. Výběrem některého z atributů totiž uživatel ihned získá statistický přehled výskytu jeho různých hodnot s možností rychlého (i negativního) filtrování dle dané hodnoty.

Bezpečnostní události jsou v systému ELISA vyhodnocovány na dvou úrovních:

- na vstupu při prvotním zpracování událostí
  - detekce výskytu konkrétních událostí
  - korelace mezi událostmi
    - opakované výskyty
    - relace mezi různými událostmi
    - kontextové korelace
    - „first“ události apod.
- definovanými periodickými dotazy do databáze
  - statistické anomálie

Hlavními vstupními kanály systému ELISA jsou:

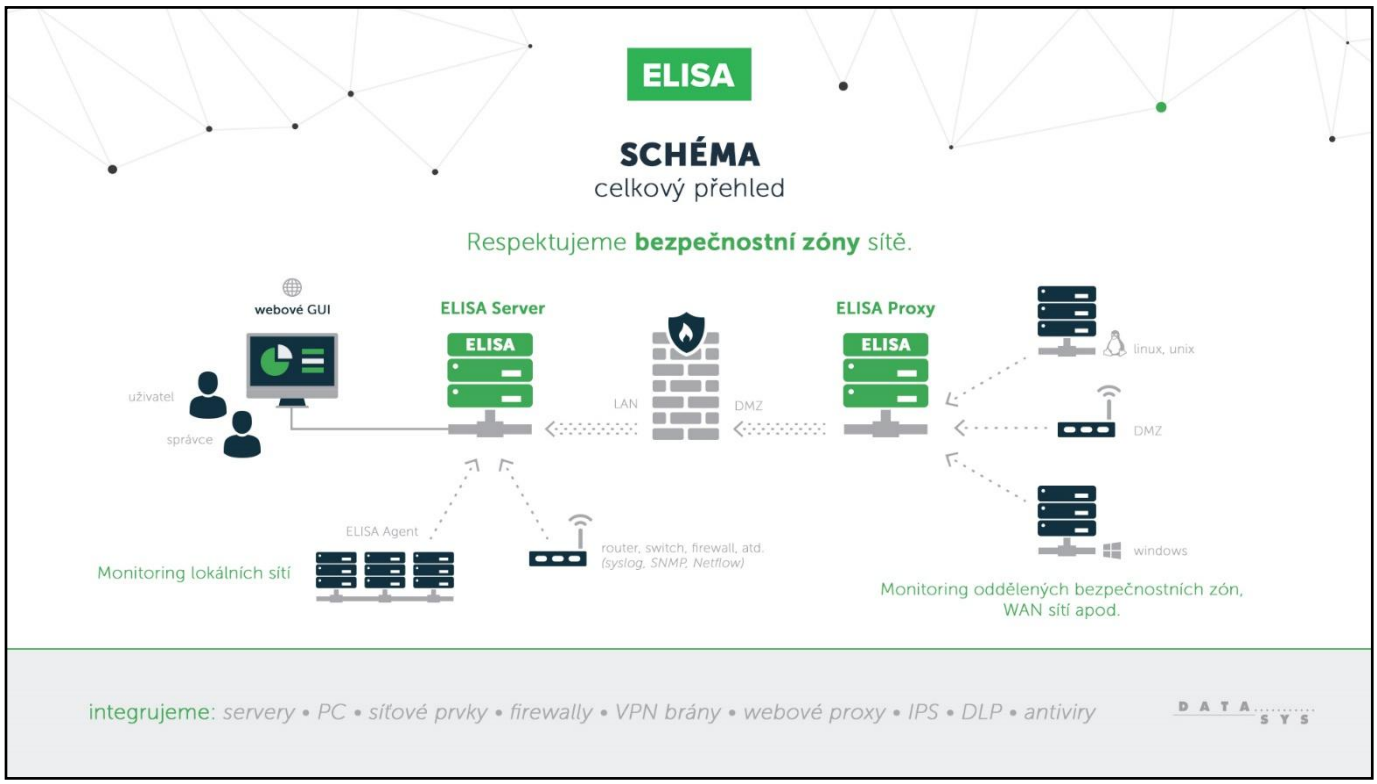
- binární protokol s podporou TLS šifrování pro přenos strukturovaných událostí (NXlog agent)
- syslog (udp i tcp)
- SNMP trapy
- netflow

Doprovodný nástroj ***NXlog*** nebo jeho klon ***DATASYS DSlog*** je určen k instalaci na monitorované systémy, které nedokáží záznamy z logů zpracovat a odeslat autonomně. Agent podporuje sběr událostí z textových logů, windows eventlogů, různých typů strukturovaných logů (CSV, j2log a dalších) a z tabulek relačních databází.

Význačné vlastnosti agenta NXlog[1]:

- multiplatformní a nenáročný na zdroje
- vytváří buffer událostí v případě nedostupnosti centrálního systému ELISA
- pamatuje si pozici již zpracovaných událostí i po restartu
- podporuje rotované log soubory, různé typy kódování a víceřádkové záznamy
- umožňuje filtrování a korelace událostí už na monitorovaném systému
- podporuje přenos strukturovaných záznamů v binárním formátu a šifrovaný přenos (SSL)

Pro získání přehledu o logické architektuře sběru dat v ELISA doporučujeme shlédnout produktové video https://youtu.be/fRpc9fgWdiw .



Bezpečnostní dohled je v systému ELISA, realizován těmito komponentami:

- **ELISA Log Manager**
  - Zajišťuje sběr logů zejména těmito mechanismy:
    - Příjem událostí ze síťových zařízení protokoly syslog, SNMP Trap, netflow
    - Načítání událostí z windows eventlogů a různě formátovaných textových logů pomocí multiplatformního agenta nebo i vzdáleně bez agenta[2]
    - Získávání logů přes http/s, ftp/s, sftp, scp, ssh, nfs, cifs, atd.
    - Načítání logů z databázových[3] tabulek, CheckPoint LEA, VMware API apod.

---

[1] Součástí dodávky licence produktu „ELISA Log Manager“ je neomezená licence pro užívání programového vybavení „NXlog Enterprise Edition“. Detailní popis jeho vlastností: http://nxlog.co/products/nxlog-enterprise-edition .

[2] Podpora „Microsoft EventLog API“ a „Microsoft Windows Event Forwarding“. Podpora formátů CEF, SDEE apod.

[3] Obecně podporujeme jakoukoli DB přístupnou přes ODBC.

- Provádí zpracování logů a jejich uložení v prokazatelně nezměněné podobě
  - Filtrování, parsování, transformace a normalizace atributů
  - Kryptografická signatura RAW formátu logu

- **ELISA Security Manager**
  - Zajišťuje obohacování logů o související informace z dalších zdrojů
  - Vykonává persistentní korelace událostí v časovém okně i několika měsíců pro automatickou alarmování potenciálních bezpečnostních incidentů
  - Provádí výpočet „Risc Score“ formulí ASSET_VALUE*SEVERITY*RELIABILITY s výslednými hodnotami v rozsahu 0 až 100, přičemž hodnotu aktiva lze definovat na úrovni zařízení
  - Poskytuje přednastavená korelační pravidla, která řeší klasické hrozby a bezpečnostní rizika a pracují s generalizovanou víceúrovňovou kategorizací, takže při správné konfiguraci parserů dat zůstávají detekční pravidla funkční i po výměně firewallu, AV systému apod.

- **ELISA Change Auditor**
  - Detekce a protokolování změn v konfiguracích serverů a zařízení
    - File Integrity Monitoring
    - Registry Integrity Monitoring
    - Protokolování rozdílů v různých exportech konfigurací
    - Protokolování změn provedených ve VMware vCenter

Nástroj ELISA podporuje[4] integraci i s dalšími v ČR rozšířenými bezpečnostními nástroji, například:
- FLOWMON pro detekci anomálií v síťové komunikaci
- NetSHIELD pro detekci a blokování neautorizovaných zařízení v síti
- OpenVAS nebo Greenbone Security Manager pro aktivní nalézání zranitelností v síti

Přehled požadavků na síťovou aplikaci typu klient/server

V souladu s požadavkem Zadavatele uvádíme v této kapitole souhrn k požadavkům na integraci nabízeného řešení do prostředí Zadavatele:

a. Navržené centrální úložiště logů je navrženo v dvouvrstvé architektuře typu klient/server a veškerý HW je součástí dodávky.
b. Veškerý potřebný HW je součástí dodávky. Jedná se o jeden 2U server s redundantním napájením s příkonem 750 W. Doporučujeme 2x připojení do datové sítě 10/100/1000Mbps.
c. Veškerý potřebný SW je součástí dodávky. Pro zálohování konfigurace doporučujeme alokovat 1GB úložného prostoru (100 MB denně). Pro případné zálohování dat nutno uvažovat až 40 TB úložného prostoru (až 200 GB denně).
d. Nabízené řešení neklade žádné specifické HW požadavky na klientskou stanici nad rámec pohodlného používání webového prohlížeče, viz též následující bod.
e. Nabízené řešení neklade žádné specifické SW požadavky na klientskou stanici s výjimkou požadavku na aktuální verzi některého z podporovaných webových prohlížečů Google Chrome, Microsoft Edge nebo Mozilla Firefox.
f. Požadavky na síťovou komunikaci:

[4] Uvádíme jen vzorové příklady pokročilejších integrací, díky podpoře standardních protokolů a průmyslových standardů podporuje ELISA na úrovni zpracování bezpečnostních alarmů integraci prakticky jakéhokoli nástroje.

Výklad použitých termínů:

- ELISA Server – centrální log management server
- Administrátoři – pracovníci provádějící konfiguraci LM
- Operátoři – uživatelé využívající analytické rozhraní
- Servery – koncová zařízení s NXlog agentem
- Ostatní zařízení – koncová zařízení, zasílají události syslog protokolem, resp. SNMP Trapy

Výklad komunikačních protokolů:

- 514/udp, 514/tcp – standardní syslog a syslog přes TCP (garantované doručení)
- 10443/tcp – aktualizace konfigurace NXlog agenta
- 10514/tcp – proprietární přenosový protokol NXlog
- 162/udp – SNMP Trapy
- 22/tcp, 443/tcp– ssh a https, přístup k uživatelským a administračním rozhraním

Následující tabulka zachycuje základní požadavky na komunikaci pro ***monitoring serverů a zařízení***:

Zdroj	**Cíl**	**Protokol**	**Poznámka**
Administrátoři	ELISA Server	22/tcp, 443/tcp	
Operátoři	ELISA Server	443/tcp	
Servery	ELISA Server	10443/tcp, 10514/tcp	
Ostatní zařízení	ELISA Server	514/tcp, 514/udp, 162/udp	

Následující tabulka zachycuje požadavky na komunikaci pro ***překlad adres, synchronizaci času, zasílání notifikací emailem a integrovanou autentizaci*** vůči Active Directory:

Zdroj	**Cíl**	**Protokol**
ELISA Server	AD servery	389/tcp, 636/tcp (pro GC 3268/tcp, 3269/tcp)
ELISA Server	SMTP server	25/tcp
ELISA Server	DNS servery	53/udp
ELISA Server	NTP servery	123/udp

Poznámka: Konektivita do sítě Internet není vyžadována nad rámec občasného nebo automatizovaného provádění aktualizací nástroje.

g. Nabízené řešení nevyžaduje dodání software a hardware třetích stran Zadavatelem

Požadavek	Splňuje (Ano / Ne)	Poznámky
Základní požadavky		
Zařízení pro centrální sběr a management logů ze síťových a bezpečnostních zařízení, serverů a stanic kupujícího, které splňuje/umožňuje:	Ano	
• požadavky zákona o kybernetické bezpečnosti a ČSN ISO 27001 pro ukládání auditních záznamů. Splnění požadavků normy ISO 27001:2013 na pořizování auditních záznamů prokázané certifikátem (či jiným obdobným dokladem) vydaným k tomu autorizovanou osobou.	Ano	K naší nabídce přikládáme vyjádření certifikovaného auditora. Nástroj ELISA je využíván v několika VIS a v jednom případě i KII, který úspěšně prošel externím auditem.
• centrální přehled s grafickou prezentací	Ano	
• možnost korelace událostí	Ano	
• možnost sjednocení formátu logů	Ano	
• licenční podmínky bez omezení na počet zařízení ani na počet přijatých zpráv za sekundu	Ano	
• podporu pro clusterový provoz	Ano	
Zařízení musí být dodáno kompletní, nové (nepoužité, nerepasované, ne starší než 12 měsíců).	Ano	
Obecné parametry		
zpracování událostí z různých zdrojů logů napříč výrobci aplikací, operačních systémů, síťového a bezpečnostního hardware	Ano	
standardizace přijatých logů do jednotného formátu a rozdělení (parserování) zpráv dle typu dílčí informace zprávy	Ano	
možnost dopsání parseru pro zařízení aktuálně nepodporované výrobcem bez nutnosti spolupráce s výrobcem nebo dodavatelem nabízeného systému	Ano	
automatická indexace rozdělených (parsovaných) zpráv pro rychlé vyhledávání	Ano	
ochrana před mazáním nebo modifikací uložených událostí	Ano	
vyhledávání událostí bez nutnosti programování	Ano	
grafické znázornění událostí s možností zobrazení TOP událostí nad veškerými daty za určité období	Ano	
automatické doplňování GeoIP informací k událostem	Ano	
automatické doplňování reverzních DNS záznamů k IP adresám	Ano	
možnost předcházet ztrátě záznamů v provozních krátkodobých „špičkách“ (v rozsahu řádově minut) použitím vyrovnávací paměti	Ano	Nastavitelná velikost vyrovnávací paměti.
reportovací nástroj s možností vlastních úprav a vytvoření nových pohledů	Ano	
konfigurační a systémové rozhraní, nápověda k systému a on-line dokumentace v českém jazyce	Ano	
čistá kapacita úložného prostoru dostupná pro uložení dat musí být minimálně 40 TB	Ano	12x 4 TB disk v RAID6

možnost vytažení/poruchy dvou libovolných disků bez ztráty dat a vlivu na funkčnost řešení (tento stav nesmí ovlivnit požadovanou kapacitu úložiště)	Ano	12x 4 TB disk v RAID6
možnost monitoringu stavu systému a upozornění formou SMTP při překročení prahových hodnot nebo chybě systému	Ano	
jednotná centrální webová konzole pro přístup k logům, upozorněním, 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	
uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému	Ano	
možnost ověření uživatele systému skrze externí LDAP	Ano	Včetně AD
HW parametry:		
zařízení obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislé na dalších systémech	Ano	
podpora HW RAID s cache min. 2 GB, která je zálohována baterií nebo jako flash paměť	Ano	
Zařízení zahrnuje minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech (rychlost minimálně 7200 otáček / 1 minutu)	Ano	
minimálně 2× 1Gbit LAN porty a 1× dedikovaný port pro management HW	Ano	
zařízení musí obsahovat systém pro vzdálenou správu serveru včetně případné potřebné licence (např. HP iLO, Dell iDrac apod.)	Ano	
SW parametry:		
zařízení musí být plně konfigurovatelné z webové konzole (tzn., že není nutná editace konfiguračních souborů)	Ano	
průměrný příjem min. 6000 událostí za sekundu	Ano	
možnost uživatelské konfigurace vlastních parserů pomocí vizuálního programovacího jazyka ve webové konzoli, vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod), vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku	Ano	I po uložení je takto sestavený parser prezentován graficky a lze jej vizuálním programovacím jazykem upravovat.
konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeolP informace a identifikace výrobce zařízení podle MAC adresy	Ano	
k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům musí být možné přidat značky či popis, který označuje např. umístění zařízení a jeho typ či kritičnost v celé soustavě	Ano	
přidávané značky jsou ukládány s každou přijatou událostí a na základě této značky je možné definovat	Ano	

datový filtr nebo omezit oprávnění uživatelů systému k jednotlivým událostem		
musí podporovat cluster o dvou a více zařízeních v režimu active/active	Ano	
systém musí splňovat podmínku, že v clusteru jsou automaticky prohledávána všechna data na všech zařízeních (z důvodu zrychlení vyhledávání)	Ano	
systém musí umožnit rozšíření kapacity a výkonu řešení formou přidání dalšího zařízení do clusteru	Ano	
v případě rozšíření clusteru musí sledovaná zařízení odesílat události pouze na jednu virtuální clusterovou adresu (synchronizaci událostí mezi cluster jednotkami si systém řídí automaticky)	Ano	
systém musí být schopen na základě zadaných podmínek (pokud jsou v přijatých datech tyto podmínky splněny) vygenerovat upozornění	Ano	
text upozornění může správce definovat s proměnnými z přijaté rozparsované události	Ano	
konfigurace upozornění se musí definovat pomocí vizuálního programovacího jazyka, Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku	Ano	
v upozornění je možné využít i značky (např. zašli upozornění v případě, že se událost stala na kritickém zařízení v lokalitě hlavní serverovny)	Ano	
pro sběr událostí z Microsoft prostředí je možné použít i SW aplikaci instalovanou přímo v koncovém systému (agent), která zajistí sběr událostí z interních logů i souborových logů	Ano	Součástí nabízeného řešení je počtem instalací neomezená licence NXlog Enterprise Edition.
agent musí podporovat nastavení filtrace odesílaných událostí, která je definována z webové konzole zařízení (z jednotného ovládacího prostředí)	Ano	
filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z webové konzole (vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku)	Ano	Analogicky jako parser.
tento agent musí být centrálně spravovatelný a aktualizovatelný přímo z webové konzole systému (nezávislost na Group Policy)	Ano	
agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.)	Ano	
agent musí být schopen překlenout krátkodobý výpadek spojení s centrálním úložištěm logů bez ztráty vygenerovaných událostí	Ano	S využitím lokálního bufferu.
centrální úložiště logů musí s aplikacemi komunikovat šifrovaně	Ano	
windows agent musí podporovat sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole nastavit i sběr všech ostatních logů	Ano	

ve složce Protokoly aplikací a služeb		
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 aplikace (agenta) nesmí být licenčně omezen	Ano	

Specifikace dalších požadavků

Níže uvedené požadavky týkající se dodávaného centrální úložiště logů (dále také *„zařízení"*) jsou blíže uvedeny ve vzoru kupní smlouvy, která činí přílohu č. 4 zadávací dokumentace.

Požadavky na implementaci:		
asistence či možnost konzultace na dálku při instalaci zařízení	Ano	
asistence či možnost konzultace na dálku při případné instalaci klientů na servery a koncové stanice	Ano	
asistence či možnost konzultace na dálku při konfiguraci jednotlivých zařízení pro sběr log záznamů	Ano	
validace příjmu jednotlivých log záznamů z podporovaných zařízení a identifikace případných potřebných úprav parsovacích pravidel	Ano	
proškolení správců systému z hlediska instalace a obecného používání zařízení	Ano	

Požadavky na služby:		
60měsíční servisní podpora výrobce hardwarové části zařízení s opravou v místě instalace zařízení v režimu NBD	Ano	
60měsíční podpora výrobce softwarové části zařízení – podpora funkčnosti a bezpečnosti softwarové části a nárok na nové verze softwarové části	Ano	

Požadavky na servisní podporu:		
komunikace prostřednictvím e-mailu a telefonu v českém jazyce	Ano	
možnost vzdáleného přístupu na zařízení v případě řešení problému (nutno uzavřít smlouvu o vzdáleném přístupu)	Ano	
bezplatné dodání SW aktualizací softwarové části zařízení v rámci servisní podpory	Ano	
rozsah servisní podpory minimálně v režimu 8×5 NBD po dobu 5 let s reakcí do 2 hodin od nahlášení požadavku.	Ano	
servisní podpora musí zahrnovat: • analýzu a identifikaci příčin nahlášené vady • odstraňování vad softwarové části centrálního úložiště dat nejpozději následujícího pracovního dne po dni, ve kterém je vada nahlášena, • předávání požadavků na odstranění vady hardwarové části centrálního úložiště logů výrobci hardwarové části centrálního úložiště	Ano	

logů, a to nejpozději následujícího pracovního dne po dni, ve kterém je vada nahlášena, • podpůrné služby v rozsahu 40 hodin ročně spočívající v údržbě centrálního úložiště logů (např. konfigurace sběru dat, vytváření dashbordů či vytváření „alertovacích“ pravidel) a konzultačních službách týkajících se centrálního úložiště logů, • provádění aktualizací softwarové části centrálního úložiště logů tak, aby byl zajištěn řádný provoz centrálního úložiště logů a bezpečnost v něm obsažených dat		

Příloha č. 2

Rozklad kupní ceny a ceny servisní podpory

	Položka (popis položky)	Počet MJ	Cena MJ (Kč bez DPH)	Cena celkem (Kč bez DPH)	DPH (Kč)	Cena celkem (Kč vč. DPH
1	Centrální úložiště logů včetně licenčních oprávněn.	1	965 250,00	965 250,00	202 702,50	1 167 952,50
3	Dodávka a implementace centrálního úložiště logů (v rozsahu dle smlouvy).		123 120,00	123 120,00	25 855,20	148 975,20
4	Školení (v rozsahu dle smlouvy).		10 790,00	10 790,00	2 265,90	13 055,90
5	Servisní podpora (1 rok)	5	179 860	899 300,00	188 853,00	1 088 153,00

Kupní cena a cena servisní podpory za dobu 5 let celkem (Kč bez DPH)	1 998 460,00
Kupní cena a cena servisní podpory za dobu 5 let celkem (Kč včetně DPH)	2 418 136,60