### SMLOUVA

**„Nákup a implementace systémového řešení pro ukládání, archivování a vyhodnocování provozních systémových událostí (logů) - SIEM a vulnerability managementu, včetně technické podpory“**

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

(dále jen „občanský zákoník“)

Ústav molekulární genetiky AV ČR, v. v. i.

se sídlem: Vídeňská 1083, Praha 4, PSČ 142 20

IČO: 68378050

DIČ: CZ68378050

zastoupen: prof. RNDr. Václavem Hořejším, CSc., ředitelem ústavu

ID datové schránky: 5h4nxm4

kontaktní osoba: Ing. Michal Sedláček

(dále jen „kupující“)

a

………

se sídlem: …….

IČO: …….

DIČ: …….

zapsaná v obchodním rejstříku u ……. soudu v ……., spisová značka …….

zastoupena: …….

bankovní spojení: …….., účet č.: …….

kontaktní osoba: …….

(dále jen „prodávající“)

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu (dále jen „smlouva“).

**I.**

**Úvodní ustanovení**

Plnění této smlouvy je veřejnou zakázkou malého rozsahu dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon“). Smlouva je uzavírána v souladu s nabídkou prodávajícího a rozhodnutím kupujícího jako zadavatele o výběru ekonomicky nejvýhodnější nabídky.

**II.**

**Předmět smlouvy**

1. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu řádně, ve sjednaném termínu, na sjednaném místě a v požadované kvalitě řešení pro ukládání, archivování a vyhodnocování provozních systémových událostí (logů) – SIEM a vulnerability managementu (dále jen „řešení SIEM“, „řešení“ nebo „zboží“). Rozsah dodávky řešení SIEM a podmínky jejího plnění jsou podrobně upraveny v „Technické specifikaci řešení vytvořené kupujícím“, která tvoří přílohu č. 1 této smlouvy a v „Technické specifikaci řešení vytvořené prodávajícím“, která tvoří přílohu č. 5 této smlouvy. V případě, kdy „Technická specifikace řešení vytvořená prodávajícím“ bude obsahovat pro kupujícího výhodnější podmínky, má přednost před „Technickou specifikací řešení vytvořenou kupujícím“.

2. Součástí plnění předmětu smlouvy je dále závazek prodávajícího provést:

a) Analýzu k implementaci řešení SIEM před dodáním řešení SIEM kupujícímu. Prodávající se seznámí s architekturou počítačové sítě kupujícího. Výstupem této analýzy bude Zpráva o implementaci řešení SIEM, která bude obsahovat:

i) způsob zasílání logů do řešení SIEM minimálně z 15 zdrojů typu: síťové přepínače, servery Windows, servery Linux, databáze, poštovní systém Exchange, antispam, antivirus, monitorovací síťové řešení, IPS/IDS, aplikační firewall, disková pole, servery;

ii) způsob iniciálního nastavení alarmů, reportů, rolí a uživatelů;

iii) doporučení činnosti k provozování a údržbě řešení SIEM kupujícím.

b) Implementaci (instalaci a konfiguraci) řešení SIEM do provozu v souladu s kupujícím odsouhlasenou Zprávou o implementaci řešení SIEM a vypracování dokumentace o provedené implementaci řešení SIEM. Nastavení řešení SIEM provede prodávající za přítomnosti zástupců kupujícího a v souladu se Zprávou o implementaci řešení SIEM.

c) Pilotní provoz řešení SIEM po provedení implementace řešení SIEM. Cílem pilotního provozu je ověřit funkcionalitu řešení SIEM. Na základě zjištěných vad a požadavků kupujícího na úpravy budou prodávajícím provedeny finální úpravy obsahu a technického nastavení řešení SIEM. Prodávající je povinen upozornit kupujícího na nevhodnost jeho požadavků. Výstupem pilotního provozu bude řešení vhodné pro ostrý provoz a Zpráva o průběhu pilotního provozu. Zpráva bude obsahovat zhodnocení průběhu pilotního provozu.

d) Podporu řešení SIEM (dále jen „podpora řešení SIEM“) na 2 roky od okamžiku zahájení ostrého provozu, spočívající v poskytování:

e) aktualizace SW vybavení řešení SIEM (např. nové definice, nové verze SW), podpora při řešení technických problémů,

f) SLA - Servisní a poradenská podpora provozu řešení SIEM při řešení provozních problémů a vyhodnocování událostí (dále jen „servisní a poradenská podpora řešení SIEM“) na dobu 5 měsíců od okamžiku zahájení ostrého provozu:

i) obsluha zařízení SIEM,

ii) garance zahájení prací následující pracovní den po nahlášení,

iii) hlášení požadavků v režimu 9x5 (9 hodin denně a 5 dnů v týdnu, v pracovní době od 8:00 do 17:00 hod), hlášené požadavky mimo uvedenou pracovní dobu budou považovány za nahlášené bezprostředně následující pracovní den, nastavování zdrojů logů, generování výstupů pro reporty, sestavování dotazů a korelačních pravidel,

iv) reakční doba do 4/12/48 hodin od nahlášení požadavku/poruchy (oznámení ze strany prodávajícího, kdo bude řešit požadavek a zahájení odstraňování); podrobně viz příloha č. 1 smlouvy „Technická specifikace řešení vytvořená kupujícím“,

v) nahlášení požadavku bude možné provádět telefonicky, elektronickou poštou nebo přes rozhraní Helpdesk systému prodávajícího,

vi) pokud kupující nestanoví jinak, je prodávající povinen vyřešit požadavek kupujícího do 3 pracovních dnů od jeho nahlášení.

vii) v rámci paušální ceny za 1 měsíc servisní a poradenské podpory má kupující nárok na 20 hodin prací).

viii) proaktivní dohled ze servisního centra prodávajícího v režimu 24x7 (24 hodin denně a 7 dnů v týdnu), zasílání upozornění a vyhledávání událostí.

g) Školení na technologii SIEM pro 3 osoby kupujícího v rozsahu 5 pracovních dní, a to v místě plnění předmětu smlouvy, příp. dle dohody smluvních stran, a to v termínu dle požadavku kupujícího.

3. Předmětem této smlouvy je dále závazek kupujícího plnění uvedené v odst. 1 a 2 (dále také jen „plnění“) převzít, tam kde to povaha plnění umožňuje, a zaplatit za něj cenu uvedenou v příloze č. 3 této smlouvy „Kalkulace ceny“.

**III.**

**Doba, místo a způsob plnění**

1. Prodávající se zavazuje plnit předmět smlouvy postupně v souladu s přílohou č. 2 této smlouvy „Harmonogram plnění“.

2. Místem plnění je Biotechnologické a biomedicínské centrum AV ČR a UK ve Vestci u Prahy, Průmyslová 595, 252 50 Vestec.

3. O předání předmětu smlouvy či jeho části jsou prodávající a kupující povinni sepsat předávací protokol. V případě, že předávaný předmět smlouvy či jeho část neobsahuje vady a nedodělky sepíší smluvní strany akceptační protokol, resp. závěrečný akceptační protokol dle čl. V. této smlouvy.

4. Nebezpečí škody na zboží přechází na kupujícího podpisem předávacího protokolu oběma smluvními stranami. Vlastnické právo ke zboží nabývá kupující uhrazením jeho ceny.

**IV.**

**Cena a platební podmínky**

1. Podrobná kalkulace celkové ceny je uvedena v příloze č. 3 této smlouvy „Kalkulace ceny“.

2. Celková cena zahrnuje veškeré náklady prodávajícího nutné nebo související s řádným plněním předmětu dle této smlouvy a jejích příloh. Žádné další náklady nebudou prodávajícímu uhrazeny. Cena bude hrazena bez poskytování záloh.

3. Celková cena ve výši bez DPH je nepřekročitelná. Na faktuře vystavené prodávajícím bude uvedená kupní cena s DPH ve výši stanovené dle platných právních předpisů. Při změně sazby DPH není třeba uzavírat dodatek k této smlouvě.

4. Faktura prodávajícího musí obsahovat veškeré náležitosti dle občanského zákoníku a dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Přílohou faktury musí být kopie příslušného akceptačního či závěrečného akceptačního protokolu dle čl. V. odst. 6. této smlouvy.

5. V případě, že faktura nebude mít stanovené náležitosti a přílohy nebo bude obsahovat chybné údaje, je kupující oprávněn ji ve lhůtě její splatnosti vrátit prodávajícímu, aniž by se tím kupující dostal do prodlení s úhradou faktury. Nová lhůta splatnosti počíná běžet dnem obdržení opravené nebo nově vystavené faktury. Důvod případného vrácení faktury musí být kupujícím jednoznačně vymezen.

6. Kupující uhradí fakturu bezhotovostně převodem na účet prodávajícího do 30 dnů ode dne obdržení faktury. Zaplacením se rozumí odepsání finanční částky z účtu kupujícího ve prospěch účtu prodávajícího.

**V.**

**Předávací a akceptační procedura**

1. Předání a převzetí jednotlivých částí předmětu smlouvy proběhne dle přílohy č. 2 této smlouvy „Harmonogram plnění“, který je pro plnění prodávajícího dle této smlouvy závazný, a to prostřednictvím akceptační procedury, která posoudí kvalitu a funkčnost provedených částí předmětu smlouvy. Výstupem akceptační procedury bude předávací protokol, akceptační protokol, resp. závěrečný akceptační protokol.

2. O předání výstupů a provedení všech činností souvisejících s plněním předmětu smlouvy bude sepsán předávací protokol, který bude obsahovat datum a popis předávaného předmětu smlouvy či jeho části a potvrdí jej podpisem osoba oprávněná jednat jménem kupujícího. Předávací protokol bude sepsán ve 2 vyhotoveních, z nichž každá smluvní strana obdrží 1 vyhotovení. Kupující je oprávněn odmítnout podepsat předávací protokol a převzít předmět smlouvy či jeho část, je-li s přihlédnutím ke všem okolnostem zřejmé, že předávaný předmět smlouvy či jeho část není v souladu s touto smlouvou či pokyny kupujícího.

3. Po podpisu předávacího protokolu je kupující oprávněn zkontrolovat, zda je předávaný předmět smlouvy či jeho část v souladu s touto smlouvou.

4. Pokud bude mít kupující po podepsání předávacího protokolu výhrady k předávanému předmětu smlouvy či jeho části, oznámí je ve lhůtě 3 pracovních dnů od předání předmětu smlouvy či jeho části listinnou nebo elektronickou formou prodávajícímu, který je povinen tyto nedostatky odstranit nejpozději do 2 pracovních dnů ode dne doručení výhrad kupujícího.

5. Po odstranění vad a nedodělků dle odst. 4 tohoto článku smlouvy předá prodávající opakovaně předmět smlouvy či jeho část kupujícímu. O předání takto opraveného předmětu smlouvy či jeho části bude opět pořízen předávací protokol a postup dle odst. 4 tohoto článku smlouvy se opakuje.

6. Postup podle odst. 3 až 5 tohoto článku smlouvy se bude opakovat až do výsledného předání předmětu smlouvy či jeho části kupujícímu bez vad a nedodělků. Má-li kupující za to, že je předmět smlouvy či jeho část bez vad a nedodělků, bude sepsán akceptační protokol nebo závěrečný akceptační protokol, který bude obsahovat datum a popis předávaného předmětu smlouvy a potvrdí jej podpisem osoba oprávněná jednat jménem kupujícího. Akceptační protokol i závěrečný akceptační protokol budou sepsány ve 2 vyhotoveních, z nichž každá smluvní strana obdrží po 1 vyhotovení.

**VI.**

**Záruka za jakost, odpovědnost za vady**

1. Prodávající odpovídá za to, že plnění má vlastnosti stanovené touto smlouvou a jejími přílohami.

2. Prodávající odpovídá za vady plnění zjištěné při jeho předání nebo v průběhu záruční doby, a to za všechny vady předmětu smlouvy existující v době předání i za vady vzniklé později. Prodávající za tímto účelem poskytuje kupujícímu záruku za jakost po záruční dobu.

3. Vadou zboží se rozumí zejména odchylka od množství, druhu či kvalitativních náležitostí zboží stanovených touto smlouvou, technickými normami či obecně závaznými právními předpisy, dále dodání jiného zboží, vady v dokladech nutných k řádnému užívání zboží a k nakládání se zbožím, poskytnutí podpory řešení SIEM a servisní a poradenské podpory řešení SIEM v rozporu s požadavky uvedenými v této smlouvě.

4. Záruční doba začíná běžet samostatně od převzetí každé části předmětu smlouvy a končí pro všechny části předmětu smlouvy 2 roky od zahájení ostrého provozu.

5. Vady zboží se kupující zavazuje v průběhu záruční doby uplatňovat písemně na adrese: …………………… nebo na e-mailu: ………………… (dále jen „kontaktní místo“).

6. Prodávající bezplatně odstraní reklamovanou vadu v místě plnění předmětu této smlouvy nejdéle do 17:00 hodin následujícího pracovního dne od nahlášení závady na uvedené e-mailové adrese. V případě nahlášení vady v nepracovní den, se za den nahlášení vady považuje první následující pracovní den.

7. O dobu odstraňování vady se prodlužuje záruční doba.

8. Reklamaci lze uplatnit nejpozději do posledního dne záruční lhůty, přičemž reklamace odeslaná kupujícím v poslední den záruční lhůty se považuje za včas uplatněnou.

9. Prodávající odstraní v záruční době reklamované vady na svůj náklad. Odmítne-li prodávající odstranit reklamované vady, případně neodstraní-li je do 10 pracovních dnů od stanoveného termínu, je kupující oprávněn odstranit vady sám nebo prostřednictvím třetího subjektu a náklady s tím spojené vyúčtovat prodávajícímu.

10. Uplatněním odpovědnosti za vady nejsou dotčeny nároky na náhradu škody nebo na uplatnění smluvní pokuty.

11. Prodávající podpisem této smlouvy potvrzuje, že má sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti prodávajícího za škodu způsobenou kupujícímu či třetím osobám ve výši minimálně 20.000.000,- Kč z jedné pojistné události ročně. Prodávající se zavazuje na žádost kupujícího bezodkladně, nejpozději však do 5 pracovních dnů od doručení písemné výzvy kupujícího, předložit kupujícímu pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Prodávající se zavazuje písemně informovat kupujícího o případných změnách týkajících se pojištění odpovědnosti za škodu, a to nejdéle do 5 pracovních dnů ode dne, kdy změna nastala. Prodávající se zavazuje, že pojistná smlouva dle věty první tohoto odstavce zůstane v účinnosti v tomto rozsahu po celou dobu trvání účinnosti této smlouvy.

**VII.**

**Součinnost smluvních stran**

1. Kupující má právo udílet prodávajícímu instrukce a připomínky v průběhu plnění předmětu smlouvy prodávajícím tak, aby byl předmět smlouvy proveden v souladu s oprávněnými zájmy kupujícího.

2. Kupující poskytne prodávajícímu při plnění předmětu smlouvy prodávajícím nezbytnou součinnost, zejména při provádění analýzy k implementaci řešení SIEM, při provádění implementace řešení SIEM, v průběhu pilotního provozu a při poskytnutí servisní a poradenské podpory řešení SIEM.

3. V případě potřeby změny osob odpovědných za poskytnutí služeb uvedených v příloze č. 5 této smlouvy „Technická specifikace řešení vytvořená prodávajícím“, je tato změna možná pouze se souhlasem kupujícího. Kupující tento souhlas neudělí v případě, že by po takové změně nově navržená osoba nesplňovala požadavky kupujícího uvedené v zadávacích podmínkách.

**VIII.**

**Práva duševního vlastnictví a ochrana osobních údajů**

1. Prodávající se zavazuje, že při plnění předmětu smlouvy neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví, že je plně oprávněn disponovat s právy, která touto smlouvou postupuje na kupujícího, nebo k jejichž užití poskytuje kupujícímu dle této smlouvy licenci a zavazuje se za tímto účelem zajistit řádné a nerušené užívání výstupů z plnění předmětu smlouvy (dále pro účely tohoto článku jen „dílo“) kupujícím, včetně případného zajištění dalších souhlasů a licencí od autorů děl v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“), popř. od vlastníků jiných práv duševního vlastnictví v souladu s právními předpisy. Prodávající se zavazuje, že kupujícímu uhradí veškeré náklady, výdaje, škodu a majetkovou i nemajetkovou újmu, které kupujícímu vzniknou v důsledku porušení povinností dle předchozí věty.

2. Je-li výsledkem činnosti prodávajícího dle této smlouvy anebo součástí předaného plnění dílo, které je předmětem práv autorských, práv souvisejících či předmětem práv pořizovatele k jím pořízené databázi, a nejde přitom ve smyslu odst. 3 tohoto článku o dílo anebo jeho části vytvořené jako zaměstnanecké dílo (dále pro účely tohoto článku souhrnně jen „Předměty ochrany podle autorského zákona“), náleží od okamžiku předání díla dle této smlouvy kupujícímu pro území celého světa včetně České republiky nevýhradní neomezené právo k užití těchto Předmětů ochrany podle autorského zákona, a to na dobu trvání práva k Předmětům ochrany podle autorského zákona, resp. na zákonnou dobu ochrany. Prodávající touto smlouvou poskytuje kupujícímu oprávnění k výkonu uvedeného nevýhradního práva k užití Předmětů ochrany podle autorského zákona (licence) bez časového, územního a množstevního omezení a pro všechny způsoby užití. Kupující je oprávněn Předměty ochrany podle autorského zákona užít v původní nebo zpracované či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky. Oprávnění k užití Předmětů ochrany podle autorského zákona získává kupující jako převoditelná s právem podlicence a dále postupitelná. Postoupení licence nebo její části na třetí osobu nevyžaduje souhlas prodávajícího a kupující není povinen postoupení licence nebo její části na třetí osobu prodávajícímu oznamovat. Toto právo kupujícího k Předmětům ochrany podle autorského zákona se automaticky vztahuje i na všechny nové verze, úpravy a překlady Předmětů ochrany podle autorského zákona dodané prodávajícím. Kupující není povinen výše uvedenou licenci využít. Prodávající dále poskytuje kupujícímu právo upravovat a/nebo překládat Předměty ochrany podle autorského zákona, včetně práva kupujícího zadat provedení těchto úprav a/nebo překladů třetím osobám. Dohodou smluvních stran se stanoví, že cena za užití Předmětů ochrany podle autorského zákona dle tohoto odstavce je součástí ceny dle přílohy č. 3 této smlouvy „Kalkulace ceny“.

3. Je-li výsledkem nebo součástí předaného plnění i zaměstnanecké či kolektivní dílo, které je předmětem autorských práv, práv souvisejících s právem autorským či práv pořizovatele k jím pořízené databázi, prodávající jako zaměstnavatel či osoba, z jejíhož podnětu a pod jejímž vedením je dílo vytvářeno a pod jejímž jménem je dílo uváděno na veřejnost, ke dni předání díla dle této smlouvy postupuje právo výkonu majetkových práv k dílu na kupujícího, přičemž výše odměny za postoupení je již zahrnuta v ceně dle přílohy č. 3 této smlouvy „Kalkulace ceny“. Kupující se tím stává ve vztahu ke všem částem díla i dílu jako celku vykonavatelem autorských práv majetkových v pozici zaměstnavatele se všemi souvislostmi včetně oprávnění vyplývajících z omezení osobnostních práv původních autorů v plném rozsahu dle autorského zákona, přičemž právo výkonu majetkových práv autorských získává kupující jako dále postupitelné. Kupující je tak především oprávněn dílo i jeho části bez dalšího sám jakýmkoli způsobem užít v původní, zpracované či jinak změněné podobě a udělit třetím osobám oprávnění (licenci) k výkonu práva dílo a jeho části užít. Kupující je dále oprávněn nehotové anebo nedostatečně podrobné části díla dokončit. Prodávajícímu ani původním autorům nenáleží nárok na přiměřenou dodatečnou odměnu. Kupující je oprávněn dílo anebo jeho části zveřejnit, upravovat, zpracovávat včetně překladu, spojit s jiným dílem, zařadit do díla souborného a uvádět je na veřejnost pod vlastním jménem.

4. S ohledem na to, že práva dle předchozích odstavců jsou poskytnuta na časově neomezenou dobu, je kupující oprávněn po skončení účinnosti této smlouvy zajistit poskytování servisní a poradenské podpory řešení SIEM jakýmkoli jiným dodavatelem.

5. Osobní údaje a důvěrné informace SIEM technologie, jenž je předmětem plnění dle této smlouvy, v reálném čase umožňuje analýzu bezpečnostních alertů (výstrah, logů), které generují síťová řešení a aplikace. SIEM řešení je postaveno na bázi aplikace, služeb a potřebného řešení - tento základ konzumuje záznamy bezpečnostních dat (logy) a generuje reporty. Systém SIEM mj. sleduje veškeré přístupy k datům kupujícího podle jmen uživatelů a adres IP s cílem zajistit prosazování obecných zásad na ochranu důvěrných informací a osobních údajů.

SIEM systém nepracuje s uživatelskými daty ve smyslu jejich obsahu. Jsou-li data vytvářena pro vytváření reportů a dále uchovávána jako archivní, musí být uložena na zabezpečených úložištích v prostorách a v technickém majetku kupujícího.

Důvěrnými informacemi se pro účely této smlouvy a po celou dobu trvání vzájemné spolupráce smluvních stran rozumí, bez ohledu na formu a způsob jejich sdělení či zachycení a až do doby jejich oprávněného zveřejnění, veškeré údaje nebo informace kromě osobních údajů, jež představují určitou hodnotu pro smluvní stranu a jež nejsou obecně známy jejím konkurentům a veřejnosti. Ve smyslu výše uvedeného zahrnují důvěrné informace zejména veškeré informace obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany, zejména výkresy, nákresy, vzorky, know-how, marketingové techniky a informace, ceníky, cenové politiky, obchodní metody a strategie, smlouvy a smluvní vztahy se zákazníky a dodavateli, analýzy a výzkum, počítačový software (včetně předmětových a zdrojových kódů), databázové technologie, systémy, struktury a architektury. Za důvěrné informace jsou dále dle této smlouvy považovány informace o organizační struktuře smluvní strany a další dokumenty označené jako důvěrné.

Osobními údaji se ve smyslu § 4 zákona o ochraně osobních údajů rozumí jakékoli informace týkající se určeného nebo určitelného subjektu, na základě kterých lze daný subjekt přímo či nepřímo identifikovat, a to na základě jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu, včetně citlivých údajů ve smyslu zákona o ochraně osobních údajů.

**IX.**

**Smluvní pokuty, úrok z prodlení**

1. Prodávající je povinen uhradit kupujícímu smluvní pokutu ve výši 0,05 % z celkové ceny včetně DPH dle přílohy č. 3 této smlouvy „Kalkulace ceny“ za každý započatý den prodlení v případě, že:

a) bude v prodlení s plněním jakékoliv části předmětu smlouvy,

b) bude v prodlení s odstraněním vad a nedostatků v rámci akceptační procedury dle čl. V. odst. 4 až 6 této smlouvy,

c) bude v prodlení s odstraněním reklamovaných vad podle čl. VI. odst. 6 této smlouvy,

d) bude v prodlení s plněním povinností dle čl. II. odst. 2 písm. f) bodu vi) této smlouvy.

2. Prodávající je povinen uhradit kupujícímu jednorázovou smluvní pokutu ve výši 10.000 Kč v případě, že:

a) poruší jakoukoli povinnost uvedenou v čl. VIII. této smlouvy,

b) nebude realizovat plnění osobami uvedenými v příloze č. 5 této smlouvy „Technická specifikace řešení vytvořená prodávajícím“, resp. osobami odsouhlasenými kupujícím dle čl. VII. odst. 3 této smlouvy.

3. Prodávající je povinen uhradit kupujícímu smluvní pokutu ve výši 10.000 Kč v případě:

a) prodlení s plněním povinností dle čl. II. odst. 2 písm. f) bodu iv), a to za každou započatou hodinu;

b) zjištění jakékoli jiné vady plnění dle této smlouvy, a to za každou jednotlivou vadu zvlášť.

4. V případě prodlení kupujícího se zaplacením faktury je prodávající oprávněn účtovat kupujícímu úroky z prodlení v zákonné výši z dlužné částky za každý den prodlení.

5. Zaplacením smluvní pokuty není dotčen nárok kupujícího na náhradu škody a na řádné dokončení plnění předmětu smlouvy.

**X.**

**Ukončení smlouvy, odstoupení od smlouvy**

1. Smluvní vztah vzniklý na základě této smlouvy lze ukončit těmito způsoby:

a) odstoupením od smlouvy:

i. za podmínek uvedených v občanském zákoníku v případě porušení smlouvy druhou smluvní stranou podstatným způsobem,

ii. v případech, které si smluvní strany ujednaly dále v tomto článku smlouvy,

b) dohodou smluvních stran,

c) výpovědí ze strany kupujícího, a to s dvouměsíční výpovědní lhůtou.

2. Kupující je oprávněn odstoupit od smlouvy v případě:

a) prodlení prodávajícího s plněním jakékoliv části plnění dle čl. II. této smlouvy delším než 20 dnů,

b) prodlení s odstraněním vad a nedostatků v rámci akceptační procedury dle čl. V. odst. 4 až 6 této smlouvy delším než 20 dnů,

c) prodlení s odstraněním reklamovaných vad podle čl. VI. odst. 6 této smlouvy delším než 20 dnů,

d) pokud řádně uplatní u prodávajícího své požadavky nebo připomínky v průběhu plnění předmětu smlouvy a prodávající je bez vážného důvodu neakceptuje nebo podle nich nepostupuje,

e) pokud po předání zboží zjistí, že nemá vlastnosti stanovené touto smlouvou, dokumentací k němu nebo nabídkou prodávajícího podanou ve výběrovém řízení, v němž byla jeho nabídka vybrána jako ekonomicky nejvýhodnější,

f) že prodávající nebude realizovat předmět smlouvy osobami uvedenými v příloze č. 5 této smlouvy „Technická specifikace řešení vytvořená prodávajícím“, resp. osobami odsouhlasenými kupujícím dle čl. VII. odst. 3 této smlouvy.

Kupující je oprávněn odstoupit z výše uvedených důvodů i jen pro dosud nesplněnou část předmětu plnění. V takovém případě mu náleží všechna práva k již předaným částem plnění, zejména pak práva dle čl. VIII. této smlouvy a záruka k již předaným částem předmětu plnění.

3. Prodávající je oprávněn odstoupit od smlouvy v případě prodlení kupujícího se zaplacením kupní ceny, delší než 20 dní po splatnosti.

4. Účinky odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně.

5. Odstoupením od smlouvy není dotčen případný nárok na náhradu škody.

**XI.**

**Poddodavatelé**

Prodávající je povinen zajistit a financovat veškeré případné poddodavatelské práce nutné k řádnému splnění jeho povinností dle této smlouvy a nese za ně odpovědnost v plném rozsahu. Aktuální seznam poddodavatelů (včetně identifikace služeb, které budou plnit) platný ke dni uzavření této smlouvy je uveden v příloze č. 6 této smlouvy. Jinou osobu, než která je uvedena v seznamu v této příloze, je prodávající oprávněn pověřit poskytnutím části předmětu této smlouvy pouze s předchozím písemným souhlasem kupujícího. Pokud prodávající nebude poddodavatele využívat, doloží čestné prohlášení, že plnění provede výhradně sám bez poddodavatelů.

**XII.**

**Závěrečná ustanovení**

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami. Tato smlouva nabývá účinnosti dnem uveřejnění v registru smluv. Smluvní strany souhlasí s uveřejněním této smlouvy v registru smluv, a to včetně všech údajů ve smlouvě uvedených. Zákonné důvody pro případné neuveřejnění některého údaje z této smlouvy se druhá smluvní strana zavazuje prokázat Ústavu molekulární genetiky AV ČR, v.v.i. nejpozději při uzavření této smlouvy. Smluvní strany se dohodly, že uveřejnění této smlouvy v registru smluv zajistí Ústav molekulární genetiky AV ČR., v.v.i., a to do tří dnů od uzavření smlouvy.

2. Změny a doplňky této smlouvy lze provést pouze formou písemných dodatků, podepsaných oprávněnými zástupci obou smluvních stran.

3. Obě smluvní stany podpisem této smlouvy vylučují, aby nad rámec jejích výslovných ustanovení a ustanovení jejích příloh byla jakákoliv jejich práva či povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami, resp. ze zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu této smlouvy.

4. Prodávající převzal na sebe nebezpečí změny okolností po uzavření této smlouvy, a proto mu nepřísluší domáhat se práv uvedených v § 1765 občanského zákoníku.

5. Prodávající souhlasí se zveřejněním této smlouvy.

6. Tato smlouva je vyhotovena ve 3 výtiscích, z nichž 1 obdrží prodávající a 2 obdrží kupující.

7. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha smlouvy č. 1 - Technická specifikace řešení vytvořená kupujícím

Příloha smlouvy č. 2 - Harmonogram plnění

Příloha smlouvy č. 3 - Kalkulace ceny

Příloha smlouvy č. 4 - Definice pravidelné služby

Příloha smlouvy č. 5 – Technická specifikace řešení vytvořená prodávajícím (vč. uvedení osob odpovědných za poskytnutí služeb uvedených v nabídce prodávajícího)

Příloha smlouvy č. 6 – Seznam poddodavatelů (příp. čestné prohlášení prodávajícího, že provede předmět této smlouvy bez poddodavatelů)

V Praze dne

 ....................................................... ………………………………….

 **Ústav molekulární genetiky AV ČR, v.v.i. prodávající**

zastoupen prof. RNDr. Václavem Hořejším, CSc., ředitelem

**Příloha smlouvy č. 1 - Technická specifikace řešení vytvořená kupujícím**

*Uchazeč vyplní všechny žlutě označené části. Tato příloha slouží* ***k vymezení minimálních technických požadavků zadavatele na technologii, kterou bude zajištěna služba a osvědčení jejich splnění uchazečem****. Uchazeč vyplní všechny položky sloupce 2 (např. popisem nabízeného parametru nebo jen slovem „SPLŇUJE“, pokud by byl popis stejný jako text uvedený ve sloupci Požadavek na funkcionalitu).*

**Název / typ řešení /:**  ………………………………………………

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 1 | Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE |  |
| 2 | Bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém) |  |
| 3 | Licence pro zpracování 1000 EPS s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 3000 EPS |  |
| 4 | Počet zdrojů pro sběr logů minimálně 150 |  |
| 5 | Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM |  |
| 6 | Možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku) |  |
| 7 | Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní |  |
| 8 | Možnost definovat uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům |  |
| 9 | Automatická identifikace systémů – zdrojů logů |  |
| 10 | Podpora šifrované komunikace mezi zdroji logů a SIEM |  |
| 11 | Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentifikace uživatelů |  |
| **Požadavek na funkcionalitu** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 12 | Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače Cisco, hw IBM/Lenovo a firewall FortiNet) |  |
| 13 | Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí |  |
| 14 | Automatické připojení zařízení výrobců IBM, Lenovo, Cisco a FortiNet |  |
| 15 | Podpora sběru síťových toků (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, sondy) |  |
| 16 | Řešení musí umožňovat automatické aktualizace |  |
| 17 | Webové uživatelské rozhraní pro management, analýzu a reporting |  |
| 18 | Poskytování automatického backup/recovery procesu |  |
| 19 | Poskytovat interní kontroly stavu zařízenířešení (healthcheck) a upozornění uživatele v případě problému |  |
| 20 | Možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI |  |
| 21 | Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box) |  |
| 22 | Řešení musí být dodáno jako all-in-one appliance (např. server) |  |
| 23 | Sběr logů z dalších bezpečnostních a síťových systémů (minimálně Cisco, FortiNet) |  |
| 24 | Výkonová rozšiřitelnost, přidáním podkladového HW  |  |
| 25 | Možnost rozšíření výběrů o uživatelské položky z obsahu logů |  |
| **Požadavek na funkcionalitu** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 26 | Zajištění integrity nasbíraných dat |  |
| 27 | Schopnost uchovat nejméně 5 TB dat (v komprimovaném formátu), aniž by vyžadovalo použití externích paměťových zařízení |  |
| 28 | Umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware |  |
| 29 | Near-real-time analýza událostí |  |
| 30 | Analýza dlouhodobých trendů událostí |  |
| 31 | Řešení musí být hodnocené v segmentu „leaders“ v GartnerMagicQuadrantu za minulé dva roky |  |
| 32 | Pokročilé "drill-down" dohledávání v případě potřeby |  |
| 33 | Možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení |  |
| 34 | Podpora a normalizace časových značek z různých časových zón |  |
| 35 | Sběr textových logů ze souborů |  |
| 36 | Sběr logů z databází pomocí JDBC/ODBC |  |
| 37 | Sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server |  |
| 38 | Rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd. |  |
| 39 | Způsob zadávání vyhledávání: Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy |  |
| 40 | Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí |  |
| **Požadavek na funkcionalitu** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 41 | Kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně |  |
| 42 | Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy |  |
| 43 | Korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení |  |
| 44 | Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení |  |
| 45 | Alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu |  |
| 46 | Řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán). |  |
| 47 | Vykonávání akci v závislosti na přijatém logu jako např. zaslat email |  |
| 48 | Schopnost pracovat s IP geolokacemi (botnet kanály atp.) |  |
| 49 | Generování alertu při výpadku logů z konkrétního zařízení |  |
| 50 | Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server) |  |
| 51 | Vyhodnocení chybějících sekvencí (např. služba přestala běžet) |  |

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 52 | Schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů |  |
| 53 | Schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele) |  |
| 54 | Schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů) |  |
| 55 | Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy |  |
| 56 | Nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS |  |
| 57 | Vulnerability nástroj - skener zranitelností provádí diagnostickou část analýzy zranitelností. Je propojený s databází, která obsahuje všechny informace ke kontrole systému na mezery v zabezpečení služeb a portů, anomálií ve struktuře paketu a potenciálních cest ke zranitelným programům nebo skriptům. |  |

|  |  |  |
| --- | --- | --- |
|  | **Požadavky na reporting** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 57 | Požadujeme automatické vytváření měsíčního reportu o stavu událostí na síti BIOCEV a o všech provedených změnách prodávajícím. |  |

|  |  |  |
| --- | --- | --- |
|  | **Požadavky na kvalitu služby** | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 58 | Telefonická podpora 24x7 v českém jazyce, jednotné kontaktní místo pro hlášení problémů a poruch.* U kritické poruchy / incidentu zahájit řešení do 4 hodin.
* U vážné poruchy / incidentu zahájit řešení do 12 hodin.
* U běžné poruchy / incidentu zahájit řešení do 48 hodin.
* Konzultace a poradenství v rozsahu minimálně 1MD měsíčně zdarma.
* Dostupnost služby 99 %
1. **Kritická porucha - incident**

Kritickou poruchou se ve smyslu této smlouvy rozumí stav celkové nefunkčnosti nebo nemožnosti využívání klíčových funkcionalit řešení nebo systému. Služba SOC / SIEM detekovala incident označený jako kritický a automaticky notifikuje odběratele.1. **Vážná porucha**

Vážnou poruchou se ve smyslu této smlouvy rozumí takový stav řešení či systému, kdy je některá komponenta nebo součást systému mimo provoz či neplní svoji funkci, ale systém jako celek je stále schopen alespoň omezeně poskytovat své služby či plnit svou funkcionalitu. Uživatelé mohou v takovém případě stále využívat služeb systému. Příkladem vážné poruchy bývá zpravidla výpadek některé redundantní komponenty zařízení (např. disk, řadič, zdroj, apod.) nebo celého řešení, které tvoří součást řešení. Služba SIEM detekovala incident označený jako vážný a během 12 hodin notifikuje odběratele.1. **Běžná porucha**

Běžnou poruchou se ve smyslu této smlouvy rozumí takový stav řešení nebo systému, který neodpovídá předávací dokumentaci, ale neohrožuje klíčové funkcionality řešení. Služba SIEM detekovala incident označený jako běžný a je založen požadavek na jeho řešení. |  |

|  |
| --- |
| Nabízené řešení splňuje veškeré minimální technické požadavky uvedené v příloze č. 1 vzoru smlouvy |
| ANO / NE\* |

\*nehodící se vymazat

**Příloha smlouvy č. 2 - Harmonogram plnění**

|  |  |  |
| --- | --- | --- |
| **Předmět plnění** | **Termín zahájení plnění**  | **Termín ukončení plnění / předání částí předmětu smlouvy** |
| Analýza (**Proof of concept**) k implementaci řešení SIEM | dnem účinnosti smlouvy  | do 5 pracovních dnů od účinnosti smlouvy  |
| Dodávka zařízení SIEM (HW a SW)  | - | do 10 pracovních dnů od účinnosti smlouvy |
| Implementace (instalace a konfigurace) řešení SIEM  | - | do 5 pracovních dnů od dodání řešení SIEM kupujícímu |
| Předání dokumentace o provedené implementaci kupujícímu | - | do 5 pracovních dnů od ukončení implementace řešení SIEM |
| Vystavení závěrečného akceptačního protokolu kupujícím | - | bez zbytečného odkladu po Předání dokumentace o provedené implementaci kupujícímu řešení SIEM kupujícímu |
| **Pilotní provoz**  | od 25. pracovního dne po uzavření smlouvy | 1 měsíc od zahájení pilotního provozu |
| Předání návrhu Zprávy o průběhu pilotního provozu řešení SIEM | - | do 5 pracovních dnů od ukončení pilotního provozu |
| Výhrady kupujícího ke Zprávě o průběhu pilotního provozu řešení SIEM |  | do 5 pracovních dnů od předání návrhu Zprávy o průběhu pilotního provozu řešení SIEM |
| Předání Zprávy o průběhu pilotního provozu řešení SIEM kupujícímu | - | do 2 pracovních dnů od předání výhrad kupujícího ke Zprávě o průběhu pilotního provozu |
| **Ostrý provoz – SLA****Pravidelné služby, dle katalogového listu** | den následující od ukončení pilotního provozu | - |
| Poskytnutí podpory (aktualizací) řešení SIEM  | Od dodávky řešení SIEM (software)  | 24 měsíců |
| Servisní a poradenská podpora řešení SIEM – služba proaktivního dohledu 24/7 a pravidelná správa, konfigurace a vyhodnocování událostí řešení SIEM, dle popisu v katalogovém listu Dohled a podpora nástroje SIEM | od zahájení ostrého provozu | 5 měsíců od zahájení ostrého provozu |

**Příloha smlouvy č. 3 – Kalkulace ceny**

Uchazeč vyplní všechna vyžlucená pole této přílohy

|  |  |  |  |
| --- | --- | --- | --- |
| **Položka** | **Cena v Kč bez DPH** | **Výše DPH v Kč** | **Cena v Kč vč. DPH** |
| **Analýza** k implementaci řešení SIEM a Zpráva o implementaci řešení SIEM |  |  |  |
| **Dodávka** řešení SIEM – HW appliance, včetně podpory řešení SIEM na 2 roky |  |  |  |
| **Implementace** (instalace a konfigurace) řešení SIEM |  |  |  |
| **Dokumentace** o provedené implementaci řešení SIEM |  |  |  |
| **Pilotní provoz** – 1 měsíc, včetně zprávy o průběhu pilotního provozu |  |  |  |
| **SLA servisní a poradenská podpora** řešení SIEM – služba proaktivního dohledu 24/7 a měsíční zpráva vyhodnocování událostí řešení SIEM – 5 měsíců |  |  |  |
| Školení 3 zaměstnanců zadavatele v rozsahu 5 pracovních dní  |  |  |  |
| **Celková nabídková cena** |  |  |  |

**Příloha smlouvy č. 4 - Definice pravidelné služby**

**Katalogový list**

**Dohled a podpora SIEM ve fázi pravidelných služeb**

|  |  |
| --- | --- |
| OZNAČENÍ SLUŽBY | Dohled a podpora nástroje SIEM  |
| Název služby | Správa provozu služby SIEM/SOC |
| VYMEZENÍ SLUŽBY |
| Prostředí | TESTOVACÍ a PRODUKČNÍ |
| Cílová skupina | Interní zaměstnanci, externí subjekty,  |
| Zkrácený popis služby | Proaktivní dohled a správa bezpečnostních prvků ICT infrastruktury |
| Předpokládaný rozsah hodin za jeden kalendářní měsíc | 20 |
| ROZSAH POŽADOVANÝCH ČINNOSTÍ  |
| **Obecný popis rozsahu služby**1. Provoz služeb SIEM * profylaktické činnosti, kontrola služeb (na denní bázi),
* kontrola logů (na týdenní bázi),
* kontrola monitoringu služby (na měsíční bázi),
* návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby,
* odborná technická podpora a odstraňování závad v předmětné oblasti – 1st level support (na denní bázi),
* správa licenčních pravidel

2. Správa služeb SIEM * kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (na měsíční bázi),
* údržba a zajištění dostupnosti služby SIEM
* analýza vhodnosti a potřebnosti implementace opravného balíku,
* návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli,
* implementace schválených požadavků na změnu konfigurace služby SIEM.

3. Dohled služeb SIEM* monitoring v reálném čase (úroveň 1 + 2)
* bezpečnostní dohled 24x7
* analýza incidentů 24x7
* návrhy řešení incidentů 8x5
* předschválená samostatná reakce

**Pravidelné činnosti – detailní popis**Služby 1. úroveň – Podpora, dohled a analýzy* 1. úroveň analýzy - představuje prostředí složené s Log management nástroje, SIEM nástroje, Vulnerability nástroje a Reportingu. Implementováno v prostředí informačního systému v lokalitě Odběratele
* log management
* zajištění sběru informací a konsolidace pro snadné vyhledávání a reporting
* konfigurace data retention v rámci Archivace informací
* SIEM – Security Information & Event Management
* vzdálená kontrola bezpečnostních událostí jejich investigace pro jejich klasifikaci
* eskalace a informování pověřených osob dle kompetenční a komunikační matice. Zakládání incidentů
* Open Threat Exchange – výměna anonymních informací o aktuálních hrozbách s OTX komunitou
* konfigurace log zdrojů napojených na SIEM
* vulnerability management
* průběžné sledování bezpečnostní kondice komponent informačních systémů – hardware, software, služby.
* přiřazení zranitelnosti k evidované komponentě.
* notifikace správců na zranitelnosti detekované modulem VM (vulnerability management)
* strukturovaný reporting podle norem ISO 27001 a PCI DSS.
* škálování konfigurace na specifické prostředí zákazníka.
* návrh systematických opatření
* analýza reportů
* dashboard
	+ přehled o aktuální bezpečnostní situaci v informačním systému.
	+ přehled o správě detekovaných událostí a průběhu analytických činností.
	+ přehled o kvalitě služeb bezpečnostní infrastruktury.
	+ přehled o dostupnosti služeb a systémů.

Služby 2. úrovně - Security Operation Centrum (SOC)* zajištění kvality a spolehlivosti bezpečnostních funkcí - Sleduje monitorovací infrastrukturu informačního systému zákazníka.
* sledování bezpečnostní situace – sleduje komponenty internetového prostředí a zdroje bezpečnostních informací.
* zajištění aktuálnosti – zajišťuje update detekčních metod pro identifikaci nových hrozeb a zranitelností zákazníka (minimálně 4x za rok).
* poskytování znalostí – implementuje best-practice postupy pro proces Security management zákazníka (minimálně 4x za rok).
* security Service Desk – služba v provozním režimu 8x5. On-line pracoviště smožností telefonní, e-mail komunikace přímo se Security Operátorem. Vpřípadě významných incidentů i specificky domluveným způsobem
* eskalace významných událostí na CISRT NSM Cluster, který je napojen na vládní CERT a na nejvyšší CSIRT ČR. V rámci velkých incidentů ohlášených NBÚ pomáhá v koordinaci aktivit potlačující negativní dopady na infrastrukturu ČR a infrastrukturu zákazníka.
* eskalace významných událostí ze sítě CESNET na CESNET-CERTS bezpečnostní tým.

**Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).*** správa a aktualizace provozní dokumentace v rozsahu:
	+ postupy pro provoz a správu služby,
	+ postupy pro obnovu služby ze záloh jednotlivých systémů,
* správa a aktualizace technické dokumentace v rozsahu (konzole systému):
	+ aktuální přehled infrastruktur jednotlivých systémů/aplikací služby SIEM,
	+ aktuální přehled parametrů jednotlivých aplikací SIEM,
	+ správa konfigurací předmětných služeb SIEM.
 |
| SERVICE LEVEL AGREEMENT (SLA) |
| Vyhodnocovací období  | 1 kalendářní měsíc |
| SLA PARAMETRY | Jednotka | Hodnota |  |  |
| Dostupnost | [%/měs] | 99 |  |  |
| Provozní doba zaručená | [hod-hod] | 00–24 (7x24) |  |  |
| Max. doba výpadku | [hod] | 4 |  |  |
| Max. doba nedostupnosti dat | [hod] | 4 |  |  |
| Max. doba servisní odezvy | [min] | 30 |  |  |
| Odstranění výpadku – A | [hod] | 4 |  |  |
| Odstranění výpadku – B | [dny] | 0,5 |  |  |
| Odstranění výpadku – C | [dny] | 2 |  |  |
| Upřesnění kategorií incidentů a závad (zpřesnění globálních definic daných servisní smlouvou) |
| Kategorie A | Nedostupnost služby SIEM, zejména:Nedochází ke sběru událostí, neběží monitoring v reálném čase. |
| Kategorie B | Závada nebo výpadek části služby SIEM, které způsobí sníženou dostupnost služby, avšak nezpůsobí celkovou nedostupnost služby SIEM. Např. nelze spravovat zdroje SIEM, systém nemá funkční analýzu útoků.  |
| Kategorie C | Ostatní závady nespadající do kategorie A nebo B, např. nefungují reporty. |
| Způsob kontroly  |
| Do dostupnosti jsou počítány pouze incidenty typu A, incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují.Měření parametrů služby budou prováděna v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost služeb systému elektronické pošty.  |
| PODMÍNKY A OMEZENÍ SLUŽBY |
| Měrná jednotka provozu služby | Počet EPS, tzv. Events Per Second (událostí za vteřinu) a počet zařízení napojených do SIEM |
| Limit objemu služby | 1000 EPS |

**Příloha smlouvy č. 5 - Technická specifikace řešení vytvořená prodávajícím (vč. uvedení osob odpovědných za poskytnutí služeb uvedených v nabídce prodávajícího)**

**Příloha smlouvy č. 6 – Seznam poddodavatelů (příp. čestné prohlášení prodávajícího, že provede předmět této smlouvy bez poddodavatelů) vč. vymezení části plnění realizovaných prostřednictvím poddodavatelů**