SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „občanský zákoník“)

Česká zemědělská univerzita v Praze
se sídlem: Kamýcká 129, 165 00 Praha – Suchdol
IČO: 60460709
DIČ: CZ60460709
zastoupená: Ing. Jakubem Kleindienstem, kvestorem
(dále jen „objednatel“ nebo „ČZU“)

a

TOTAL SERVICE a.s.
IČO: 25618067
DIČ: CZ25618067
Zastoupená: Ing. Janem Navrátilem, členem představenstva
(dále jen „poskytovatel”)

(společně „smluvní strany“)

uzavírají na základě výsledku zadávacího řízení k plnění veřejné zakázky s názvem „**Zajištění bezpečnostních služeb Qradar na ČZU**“ zadávané v rámci zavedeného dynamického nákupního systému „Dynamický nákupní systém na dodávky serverové infrastruktury a síťových prvků – II.“ tuto smlouvu o poskytování služeb (dále jen „smlouva“).

I.
Předmět smlouvy

1. Předmětem této smlouvy je na jedné straně závazek poskytovatele migrace dat ze stávajícího systému na nové řešení SIEM a zajištění podpory v souladu s přílohou č. 1 této smlouvy (dále jen „služby“).

2. Předmětem smlouvy na straně druhé je pak závazek ČZU za poskytnuté služby poskytovateli zaplatit dohodnutou cenu ve výši a způsobem stanoveným v této smlouvě.

II.
Způsob plnění smlouvy

1. Smluvní strany sjednávají, že poskytování služeb bude uskutečňováno na základě jednotlivých dílčích požadavků ČZU. Tyto požadavky budou předem projednány určenými zástupci smluvních stran, a na základě tohoto projednání vystaví ČZU písemnou objednávku k poskytnutí konkrétních služeb (dále jen „objednávka“).

2. V souladu s povinnostmi poskytovatele dle článku III. níže bude objednávka obsahovat následující údaje:
   - označení požadované služby v souladu s přílohou č. 1 a č. 3 této smlouvy,
   - cenu za poskytování služeb dle dané objednávky v souladu s přílohou č. 3 této smlouvy,

- označení osoby, která objednávku vystavila.

3. Objednávka bude zaslána poskytovateli elektronicky e-mailem na adresu kontaktní osoby poskytovatele, Bc. Jiří Hazuka, e-mail: jhazuka@totalservice.cz, a poskytovatelem potvrzena do 48 hodin e-mailem na adresu kontaktní osoby ČZU dle čl. III. odst. 2 této smlouvy.

III.
Povinnosti poskytovatele

1. Zajistit a poskytovat služby dle předmětu této smlouvy, a to především zajistit migraci ze stávajícího systému na nové řešení SIEM, na stejné technologické platformě a dodávka nástroje na správu agendy formou služby, včetně následné poskytování odborných technických a dohledových služeb nad platformou SIEM, včetně souvisejícího odborného poradenství. Vymezení služeb a podmínky jejich provádění jsou blíže specifikovány v příloze č. 1 této smlouvy.

2. Při výkonu služeb se řídit pokyny pověřených zaměstnanců ČZU a spolupracovat s nimi dle jejich pokynů a požadavků. Pověřenými zaměstnanci v rámci plnění předmětu smlouvy jsou:

    a. Jan Bureš, tel: +420 724 289 356, email: buresj@rektorat.czu.cz

3. Seznamovat pověřené zaměstnance ČZU s výsledky služeb uskutečňovaných na základě jednotlivých objednávek, a to formou dílčích písemných zpráv, dle čl. II., odst. 2. této smlouvy.

4. Nejpozději do 10 dnů od ukončení aktivity seznámit s výsledky služeb pověřené zaměstnance ČZU prostřednictvím shrnující písemné zprávy o poskytnutých službách, která bude obsahovat informace získané z provedených analýz.

5. Poskytovatel je povinen vytvořit realizační tým dle přílohy č. 2 této smlouvy a při plnění předmětu smlouvy využít výhradně tyto členy realizačního týmu, změny realizačního týmu musí proběhnout v souladu s čl. VIII. odst. 5 této smlouvy.

6. Poskytovatel podpisem této smlouvy potvrzuje a prohlašuje neexistenci střetu zájmů v souladu s § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „zákon o střetu zájmů“) a tedy, že (i) není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona o střetu zájmů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba, vlastní podíl představující alespoň 25 % účasti společníka; a že (ii) žádný poddodavatel, není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona o střetu zájmů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba, vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti. Poskytovatel se zavazuje bezodkladně písemně informovat objednatele o jakékoliv změně týkající se výše uvedených prohlášení o neexistenci střetu zájmů. Nedodržení této povinnosti se považuje za hrubé porušení smlouvy, v takovém případě je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 25% ceny (bez DPH) uvedené v čl. V. odst. 1 této smlouvy. Úhradou smluvní pokuty zůstávají nedotčena práva objednatele na náhradu škody v plné výši.

7. Poskytovatel podpisem této smlouvy potvrzuje a prohlašuje, pro potřeby naplňování požadavků na ochranu finančních zájmů EU ve smyslu čl. 22 Nařízení Evropského parlamentu a Rady (EU) č. 2021/241, konkrétně za účelem předcházení riziku střetu zájmů, že je u něj a jeho zainteresovaných osob vyloučen střet zájmů ve smyslu čl. 61 Nařízení č. 2018/1046 Evropského parlamentu a Rady (EU, Euratom) ze dne 18. července 2018, kterým se stanoví finanční pravidla pro

souhrnný rozpočet Unie (Finanční nařízení) a Sdělení Komise č. 2021/C 121/01 Pokyny k zabránění střetu zájmů a jeho řešení podle Finančního nařízení, ve smyslu Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, a to ve vztahu k zainteresovaným osobám, tj. k objednateli a jeho zaměstnancům, příp. také u dotčených subjektů dotačního orgánu, které jsou smluvním stranám ke dni podpisu této smlouvy známy. Poskytovatel se zavazuje bezodkladně písemně informovat objednatele o jakékoliv změně týkající se výše uvedeného prohlášení o neexistenci střetu zájmů. Nedodržení této povinnosti se považuje za hrubé porušení smlouvy, v takovém případě je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 25% ceny (bez DPH) uvedené v čl. V. odst. 1 této smlouvy. Úhradou smluvní pokuty zůstávají nedotčena práva objednatele na náhradu škody v plné výši.

8. Poskytovatel podpisem této smlouvy prohlašuje, že je informován o povinnostech spadajících na povinné osoby vyplývající ze zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti, ve znění pozdějších předpisů (dále jen „AML zákon“) a potvrzuje, že není politicky exponovanou osobu ve smyslu § 4 odst. 5 AML zákona, a že vůči němu Česká republika neuplatňuje mezinárodní sankce podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů. Poskytovatel prohlašuje, že ustanovení předchozí věty platí i pro všechny jeho poddodavatele. Poskytovatel se zavazuje bezodkladně písemně informovat objednatele o jakékoliv změně týkající se výše uvedených prohlášení. Nedodržení této povinnosti se považuje za hrubé porušení smlouvy, v takovém případě je objednatel oprávněn účtovat poskytovateli smluvní pokutu 25% ceny (bez DPH) uvedené v čl. V. odst. 1 této smlouvy. Úhradou smluvní pokuty zůstávají nedotčena práva objednatele na náhradu škody v plné výši.

9. Poskytovatel podpisem této smlouvy prohlašuje, že splňuje podmínky dle sankčního nařízení Rady EU č. 2022/576, kterým se mění předchozí nařízení o omezujících opatřeních přijatých vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, tedy že není:
    a. ruským státním příslušníkem, fyzickou či právnickou osobou, subjektem či orgánem se sídlem v Rusku,
    b. právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmenu a), nebo
    c. poskytovatelem jednajícím jménem nebo na pokyn některého ze subjektů uvedených v písmenu a) nebo b).

10. Poskytovatel prohlašuje, že uvedené podmínky dle nařízení Rady EU č. 2022/576 splňují i jeho (i) poddodavatelé; a (ii) dodavatelé nebo subjekty, jejichž způsobilost je využívána ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Poskytovatel se zavazuje bezodkladně písemně informovat objednatele o jakékoliv změně týkající se výše uvedených prohlášení. Nedodržení této povinnosti se považuje za hrubé porušení smlouvy, v takovém případě je objednatel oprávněn účtovat poskytovateli smluvní pokutu 25% ceny (bez DPH) uvedené v čl. V. odst. 1 této smlouvy. Úhradou smluvní pokuty zůstávají nedotčena práva objednatele na náhradu škody v plné výši.

IV.
Povinnosti ČZU

1. Poskytnout potřebnou součinnost k zajištění služeb pro ČZU, zejména včasným poskytnutím dat a informací, které poskytovatel nezbytně potřebuje k plnění předmětu smlouvy.

2. Informovat poskytovatele o všech důležitých skutečnostech a změnách, které by mohly mít vliv na realizaci předmětu smlouvy.

V.
Cenové a platební podmínky

1. Odměna za poskytování služeb dle této smlouvy nepřesáhne celkovou maximální výši 40.000.000,- Kč bez DPH. Jednotkové ceny jsou uvedeny v příloze č. 3 této smlouvy. DPH bude připočtena ve výši dle platných právních předpisů. Celková výše odměny je nejvyšší přípustná a nepřekročitelná.

2. Odměna dle odst. 1. výše zahrnuje veškeré náklady poskytovatele spojené s plněním předmětu této smlouvy.

3. Odměna za služby poskytované na základě objednávek bude hrazena v české měně prostřednictvím faktur vystavovaných poskytovatelem vždy do 15 dnů od předložení dílčí písemné zprávy vztahující se ke konkrétní objednávce. Poslední faktura bude vystavena do 15 dnů od dodání shrnující písemné zprávy dle čl. III. odst. 4. této smlouvy. Faktura musí obsahovat veškeré náležitosti daňového dokladu dle platných právních předpisů.

4. Daňový doklad – faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že faktura nebude mít odpovídající náležitosti, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury objednateli.

5. Splatnost daňového dokladu (faktury) je 30 dnů ode dne jeho doručení objednateli. Fakturu je zhotovitel povinen doručit na adresu: faktury_oikt@czu.cz. Jiné doručení nebude považováno za řádné s tím, že objednateli nevznikne povinnost fakturu doručenou jiným způsobem uhradit.

VI.
Trvání smlouvy

1. Tato smlouva se uzavírá na dobu do vyčerpání maximální odměny poskytovatele dle čl. V. odst. 1. smlouvy.

2. ČZU je oprávněna tuto smlouvu vypovědět, pokud poskytovatel opakovaně poruší povinnosti dané touto smlouvou dle čl. III. této smlouvy. Výpověď je platná od prvního dne následujícího měsíce od doručení výpovědi.

3. Poskytovatel je oprávněn tuto smlouvu vypovědět, pokud ČZU opakovaně poruší povinnosti dané touto smlouvou dle čl. IV. této smlouvy. Výpověď je platná od prvního dne následujícího měsíce od doručení výpovědi.

4. Smluvní strany jsou oprávněny tuto smlouvu vypovědět i bez udání důvodu s tím, že výpovědní lhůta činí 1 měsíc od doručení výpovědi.

VII.
Sankce

1. V případě, že poskytovatel poruší své povinnosti stanovené touto smlouvou a ČZU tím vznikne škoda, je poskytovatel povinen tuto škodu na základě výzvy uhradit.

2. V případě, že ČZU poruší své povinnosti stanovené touto smlouvou a poskytovateli tím vznikne škoda, je ČZU povinna tuto škodu na základě výzvy uhradit.

VIII.
Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem podpisu smlouvy oprávněnými zástupci obou smluvních stran. Tato smlouva nabývá účinnosti v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

2. Poskytovatel bezvýhradně souhlasí se zveřejněním plného znění smlouvy tak, aby tato smlouva mohla být předmětem poskytnuté informace ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

3. Poskytovatel bezvýhradně souhlasí se zveřejněním plného znění smlouvy tak, aby tato smlouva mohla být předmětem poskytnuté informace ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Poskytovatel rovněž souhlasí se zveřejněním plného znění smlouvy dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

4. Poskytovatel bere na vědomí a souhlasí, že je osobou povinnou ve smyslu § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů. Zhotovitel je povinen plnit povinnosti vyplývající pro něho jako osobu povinnou z výše citovaného zákona.

5. Veškeré změny či doplnění smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků smlouvy.

6. Smluvní strany nejsou oprávněny postoupit, převést, ani zastavit tuto smlouvu ani jakákoli práva, povinnosti, dluhy, pohledávky nebo nároky vyplývající z této smlouvy a v souvislosti s ní bez předchozího písemného souhlasu druhé Smluvní strany.

7. Smlouva se vyhotovuje a podepisuje elektronicky.

8. Nedílnou součástí této smlouvy jsou následující přílohy:
   Příloha č. 1 – Technická specifikace,
   Příloha č. 2 – Realizační tým,
   Příloha č. 3 – Oceněný kalkulační model.

9. Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a ostatními obecně závaznými právními předpisy.

10. Smluvní strany prohlašují, že si smlouvu před jejím podpisem přečetly a s jejím obsahem bez výhrad souhlasí. Smlouva je vyjádřením jejich pravé, skutečné, svobodné a vážné vůle. Na důkaz pravosti a pravdivosti těchto prohlášení připojují oprávnění zástupci smluvních stran své vlastnoruční podpisy.

V Praze dne:

Jan Navrátil

Digitálně podepsal Jan Navrátil
Datum: 2023.12.22 14:13:35 +01'00'

…….

poskytovatel
TOTAL SERVICE a.s.
Ing. Jan Navrátil
člen představenstva

V Praze dne:

Ing. Jakub Kleindienst

Digitálně podepsal Ing. Jakub Kleindienst
Datum: 2023.12.22 11:22:48 +01'00'

…….

objednatel
Česká zemědělská univerzita v Praze
Ing. Jakub Kleindienst
kvestor

Příloha č. 3 - Technická specifikace (a současně příloha č. 1 Smlouvy)

Název

Obnova nástroje pro vyhodnocování bezpečnostních událostí včetně odborných služeb bezpečnostního monitoringu a souvisejícího poradenství

Technická specifikace

Předmětem plnění smlouvy je migrace ze stávajícího systému na nové řešení SIEM, na stejné technologické platformě a dodávka nástroje na správu agendy formou služby, včetně následné poskytování odborných technických a dohledových služeb nad platformou SIEM, včetně souvisejícího odborného poradenství a konzultací v oblasti kyberbezpečnosti.

A) Dodávka SW SIEM a plán převzetí Služeb – Poskytovatel provede:

- převzetí a kontrolu stávajících technologií;
- dodávku nových SW licencí řešení platformy SIEM;
- migrace dat ze stávajícího řešení nástroje a politik pro SIEM.

B) Zajištění provozu Služeb – Poskytovatel provede:

- KL01 - SPRÁVA PLATFORMY SIEM;
- KL02 - SLUŽBY BEZPEČNOSTNÍHO MONITORINGU
- KL03 – POSKYTOVÁNÍ AD-HOC SLUŽEB SPECIALISTŮ

C) Služby exitu

D) Společná ustanovení

E) Harmonogram plnění

A) Dodávka SW SIEM a plán převzetí Služeb

1.1 Služby převzetí

Součástí nabídky účastníka musí být navrhovaný popis a harmonogram převodu služeb na poskytovatele, tj. poskytnutí služeb Plánu převzetí služeb. Součástí této tranzice musí být minimálně:

- seznámení se s přebíranými technologiemi a jejich kontrola,
- předání dokumentace, včetně metodik,
- ověřená, případně aktualizovaná dokumentace a schémata,
- protokol o funkčnosti přístupů k technologiím (fyzický i pro management technologií),
- protokol o převzetí stávající technologie pro migraci a následná správa.

Na základě poskytovatelem navrhovaných bodů tranzice navrhne poskytovatel harmonogram tranzice v délce trvání maximálně jeden (1) měsíc od účinnosti smlouvy, tento harmonogram a popis tranzice bude součástí nabídky.

1.2 Dodávka licencí výrobce pro platformu SIEM (SW)

Dodání řešení založeného na platformě Qradar SIEM v rozsahu min.

Popis licence	Qty
QRadar Software Install License +1 Year Software Subscription and Support	1
QRadar Software Install License S&S Renewal	3
QRadar Software Node Install License+1 Year Software Subscription and Support	1
QRadar Software Node Install License S&S Renewal	3
QRadar Software Node Install License+1 Year Software Subscription and Support	1
QRadar Software Node Install License S&S Renewal	3
QRadar Event Capacity 2.5K Events Per Second License+1 Year Software Subscription and Support	1
QRadar Event Capacity 2.5K Events Per Second License S&S Renewal	3
QRadar Event Capacity 500 Events Per Second License+1 Year Software Subscription and Support	1
QRadar Event Capacity 500 Events Per Second License S&S Renewal	3
QRadar Flows Capacity 25K Flows Per Minute License+1 Year Software Subscription and Support	1
QRadar Flows Capacity 25K Flows Per Minute License S&S Renewal	3

Včetně zpracování implementační dokumentace nasazení SIEM

B) - Zajištění Služeb

Poskytovatel poskytuje Služby dle Katalogových listů v rámci paušální měsíční Služby v rozsahu:

1) KL01 – SPRÁVA PLATFORMY SIEM
2) KL02 – SLUŽBY BEZPEČNOSTNÍHO MONITORINGU
3) KL03 – POSKYTOVÁNÍ AD-HOC SLUŽEB SPECIALISTŮ

KL01 – SPRÁVA PLATFORMY SIEM

POPIS SLUŽBY

Proaktivní dohled a správa nad bezpečnostní technologií Platformy SIEM

Parametry služby

1. Měrné jednotka:
    a. SIEM, 3 000 EPS, 25 000 FPM;
2. Limit objemu služby:
    a. Poskytovatel se zavazuje ke správě Platformy SIEM v rozsahu stávajícím (dle měrné jednotky výše) až do nárůstů o max. 50%.
3. Doba provozu služby:
    a. 24x7x365.

DETAILNÍ POPIS SLUŽBY

Implementace prostředí SIEM je provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí dle Vyhlášky č. 82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění.

Správa Platformy SIEM

- Provoz zařízení SIEM,
- Profylaktické činnosti, kontrola služeb (na týdenní bázi),
- Kontrola provozních logů zařízení (na týdenní bázi),
- Návrh případných opatření s cílem předejít možným výpadkům a omezením poskytovaných služeb zařízením SIEM,
- Odborná technická podpora a odstraňování závad v předmětné oblasti,
- Správa licenčních pravidel.

1. Správa zařízení SIEM a doplňkových modulů
    - 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 Objednateli,
    - Implementace schválených požadavků na změnu konfigurace služby SIEM.

2. Konfigurace log zdrojů napojených na SIEM a doplňkových modulů
    - Vytváření DSM modulu pro neznámé zdroje v SIEM, aby bylo možné kategorizovat informace obsažené v logu (dle dohody s objednatelem),
    - Kontrola správné funkce infrastruktury a případná náprava nežádoucího stavu,
    - Přidávání Logsources (dle dohody s objednatelem).

Pravidelné činnosti – správa infrastruktury SIEM:

- Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců, případně nových verzí opravující vážné bezpečnostní chyby (na kvartální bázi),
- Analýza vhodnosti a potřebnosti implementace opravného balíku,

- Návrh opatření a postupu implementace opravného balíku ke schválení objednateli,
- Instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně),
- Implementace schválených požadavků na změnu konfigurace včetně deployment nových sond nebo jejich aktualizací,
- Škálování konfigurace na specifické prostředí objednatele.

Provoz služby:

- Komplexní monitoring všech infrastrukturních zařízení a systémů, serverů, operačních systémů, systémových služeb, databází, sítí, ale v omezeném rozsahu i klíčových aplikací a aplikačních služeb objednatele,
- Profylaktické činnosti (na týdenní bázi) – čištění nepotřebných souborů, archivace logů, kontrola čitelnosti uložených dat, tvorba reportů,
- Kontrola logů monitorovacích systémů (na denní bázi),
- Kontrola výkonnosti a performance monitoring sledovaných technologií (na týdenní bázi),
- Incident management - Odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na týdenní bázi),
- Problém management - Návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře (minimálně kvartálně nebo dle aktuální situace),
- Podpora služby v provozním režimu 24x7 s možností telefonní nebo e-mail komunikace přímo se Security Operátorem. V případě významných incidentů i specificky domluveným způsobem.

Všechny parametry služby zajišťují na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost a Integrita.

Reportování a měření	Reportování událostí probíhá 1x za tři měsíce Rozšířený reporting – požadavků od Objednatele a informace jejich plnění probíhá 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. Prezentace měsíčních reportů v rozsahu 2 hod. Report bude obsahovat minimálně následující: • Seznam patchů, hotfixů, service packů a dalších opravných balíků výrobců, případně nových verzí opravující vážné bezpečnostní chyby, • Analýza vhodnosti a potřebnosti implementace opravného balíku, • Návrh opatření a postupu implementace opravného balíku, • Seznam implementace schválených požadavků na změnu konfigurace včetně deployment nových sond nebo jejich aktualizací.

SERVICE LEVEL AGREEMENT (SLA)		
Vyhodnocovací období	1 kalendářní měsíc	
SLA PARAMETRY	Jednotka	Hodnota
Dostupnost	[%/měsíc]	Se řídí dle KL 3
Provozní doba zaručená	[hod-hod]	24x7x365
Max. doba výpadku	[hod]	Se řídí dle KL 3
Max. doba nedostupnosti dat	[hod]	Se řídí dle KL 3

Max. doba zahájení řešení incidentu / požadavku	[hod]	Se řídí dle KL 3
Odstranění výpadku A1-A2	[hod]	Se řídí dle KL3
Odstranění výpadku B3-B4	[dny]	Se řídí dle KL3
Odstranění výpadku C5	[dny]	Se řídí dle KL3

UPŘESNĚNÍ KATEGORIÍ INCIDENT	
Kategorie A1 a A2	Nedostupnost některé z klíčových technických součástí
Kategorie B3 a B4	Závada nebo výpadek části služby, které způsobí sníženou dostupnost služby, avšak nezpůsobí celkovou nedostupnost služby.
Kategorie C5	Ostatní závady nespadající do kategorie A1, A2, B3, B4

ZPŮSOB KONTROLY
Do dostupnosti jsou počítány pouze incidenty typu A1 a A2, incidenty kategorie B3, B4 a C5 se do vyhodnocení celkové dostupnosti nezahrnují.

PODMÍNKY A OMEZENÍ SLUŽBY	
Předpoklady služby	Správa prostředí je zajišťována nad SIEM nástrojem v majetku objednatele.
Výjimky služby	V případě, kdy prokazatelně došlo k výpadku služby v přímém důsledku neodborné činnosti provedené zástupci objednatele, tak je poskytovatel zproštěn veškerých negativní důsledků vyplývajících z takového výpadku, včetně vyloučení výpočtu SLA u těchto zařízení.

ZPŮSOB A ROZSAH POSKYTOVÁNÍ SLUŽEB DLE KATALOGOVÉHO LISTU 02

a) Poskytování nových verzí SIEM a opravných patchů zahrnuje následující činnosti:

- poskytování aktualizací a nových verzí SIEM;
- poskytování opravných patchů nutných pro bezchybný chod SIEM;
- poskytnutí technické podpory na HW Platformy SIEM.

b) Objednatel má nárok na veškerá zlepšení a dodatky k SIEM (zejm. upgrade nebo update SIEM) vydané během účinnosti smlouvy. Součástí poskytnutí těchto upgrade a update je též jejich testování a implementace a rozdílové školení, pokud bude potřeba s ohledem na rozsah upgrade či update.

c) Update se rozumí aktualizace SIEM formou opravných patchů, zohledňující většinou chyby nebo bezpečnostní mezery, které u předcházející verze nebyly známé včetně veškerých Dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technické dokumentace zahrnující i případné bezpečnostní pokyny související s opravným balíčkem k SIEM.

d) Upgrade se rozumí vylepšení dosavadního SIEM na vyšší výkonnost a nové funkce včetně veškerých Dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, instalačního manuálu a doporučení pro implementaci, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technické dokumentace zahrnující i případné bezpečnostní pokyny související s aktualizací komponent SIEM.

e) Součástí předmětu plnění dle tohoto Katalogového listu není nárok na poskytování nových verzí SIEM vytvořených na základě individuální objednávky objednatele, ani dokumentace k takto vytvořeným novým verzím SIEM.

f) Poskytovatel do pěti (5) pracovních dnů ode dne vydání update či upgrade oznámí oprávněné osobě objednatele uvolnění každého update i upgrade a důvod, proč k update či upgrade dochází.

g) Poskytovatel je povinen do pěti (5) pracovních dnů ode dne vydání update zabezpečit jejich neomezenou dostupnost tak, aby takový update a/nebo upgrade byl pro objednatele kdykoliv přístupný.

KL02 – SLUŽBY BEZPEČNOSTNÍHO MONITORINGU
POPIS SLUŽBY
Bezpečnostní monitoring a proaktivní dohledové služby budou poskytnuty jako komplexní a centralizovaná správa, ukládání a vyhodnocování bezpečnostních logů v nezměnitelné podobě z různých síťových aktivních prvků, sond, bezpečnostních bran, operačních systémů, databází a napojeného aplikačního software, včetně VIS systémů, a provozované formou dodavatelské služby v hybridního modelu dohledového centra kybernetické bezpečnosti (SOC – Security Operations Centra), jenž tvoří týmy L1, L2, L3 ze strany Poskytovatele a základní L0 služba na straně objednatele (8-16), a to nad SW nástroji platformy SIEM ve vlastnictví objednatele.
PARAMETRY SLUŽBY
1. Měrná jednotka: • Aktuální počet zdrojů: cca. 50 • Počet událostí k analýze: 5.000/rok (cca. 20 každý pracovní den) - role SOC Operátora • Počet událostí (incident): 1.200/rok (cca. 5 každý pracovní den) - role SOC Analytika ** 2. Limit objemu služby: • Poskytovatel se zavazuje k plnění v rozsahu stávajícím (dle měrné jednotky výše) až do nárůstů o max. 25% • *Většina napojených zdrojů logů je napojena pomocí přesměrování logů z předřazeného LogManager • **počet byl stanoven s ohledem na dosavadní praxi, jenž zahrnuje vysokou časovou náročnost s ohledem na potřeby dalšího dohledání klíčových dat. U určitých incidentů je potřeba další investigace zahrnující dohledávání dat v log a flow aktivitě, dohledávání informací z dostupných zdrojů v oblasti známých vulnerabilit a komunikace s dalšími třetími stranami pro potřeby ověření možné kompromitace nebo závadové aktivity v prostředí. 3. Doba provozu služby: • 24x7x365
DETAILNÍ POPIS SLUŽBY
Bezpečnostní monitoring je zajištěn nástrojem objednatele umožňující monitorování sítě, serverů a služeb. Nástroj poskytuje varování o potenciálních bezpečnostních incidentech, trendech a historii sítě, serverů a služeb systémů objednatele. **Provádění průběžného bezpečnostního monitoringu:** Bude zajištěn a prováděn průběžný bezpečnostní monitoring systému objednatele za účelem poskytnutí nepřetržitého dohledu nad stavem bezpečnosti systému, zajištění schopnosti proaktivní, včasné reakce na bezpečnostně relevantní události a shromažďování důkazů a podkladů pro řešení bezpečnostních incidentů. Službou budou zajištěny následující činnosti:

- analytická činnost nad bezpečnostními událostmi v systémech objednatele, hledání a nalezení příčin událostí, anomálních chování, bezpečnostních hrozeb a podobně - v současnosti komplexně označováno jako ThreatManagement,
- sledování anomálií běžného provozu vybraných aplikací a jejich vyhodnocování,
- průběžná optimalizace parametrů chování sledovacích systémů (tresholdů), označování false positive incidentů,
- kontrola vlastních bezpečnostních pravidel, systémů bezpečnostní infrastruktury,
- detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti,
- průběžný bezpečnostní audit logů (korelace, agregace, vyhodnocování a uchovávání).

Vyhledávání slabých míst:

Služba Bezpečnostní monitoring je schopna na základě prováděného průběžného monitoringu identifikovat slabá místa v systému objednatele a posoudit je z pohledu vhodnosti a dostatečnosti implementovaných bezpečnostních opatření.

V návaznosti na tyto skutečnosti bude vydávat doporučení provozovateli aplikace objednatele s cílem zajistit instalaci, implementaci nebo rekonfiguraci určených prvků, komponent, konfiguračních položek, případně jiných oblastí.

Pravidelné činnosti – analytická činnost Bezpečnostního monitoringu

- Analýza bezpečnostních incidentů v systému objednatele:
  - Posouzení incidentu z hlediska false-positives bezpečnostních incidentů,
  - Vyhodnocení příčin vzniku bezpečnostních incidentů,
  - Vyhodnocení dopadu bezpečnostních incidentů (změny v systémech / infrastruktuře, uniklá data, atd.),
  - Návrh a konzultace opatření.
- Strukturovaný reporting:
  - Reporting zjištěných bezpečnostních incidentů,
  - Reporting zjištěných zranitelností v infrastruktuře,
  - Reporting anomálií v infrastruktuře,
  - Reporting nekorektního chování infrastruktury nebo jejich částí,
  - Konzultace nad reporty.
- 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.
- Škálování konfigurace na specifické prostředí objednatele.

  Podpora služby v provozním režimu 5x8 s možností telefonní nebo e-mail komunikace přímo se Security Operátorem. V případě významných incidentu i v režimu 24/7/365.

Všechny parametry služby zajišťují na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost a Integrita.

Reportování a měření	Reportování bezpečnostních událostí probíhá 1x týdně. Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření probíhá 1x

	měsíčně. Vzdálená prezentace reportu např. formou videokonference. Prezentace měsíčních reportů v rozsahu 2 hod. Report musí obsahovat minimálně následující: • Kompletní přehled událostí za dané období (měsíc), agregovaný dle typu události a seřazený dle priorit a porovnání s předchozím obdobím, • Detailní rozbor jednotlivých událostí za dané období dle jednotlivých typů událostí a porovnání s předchozím obdobím, • Přehled nejčastějších zdrojů a cílů událostí za dané období (u událostí typu Upload a High Transfer také přehled podle množství přenesených dat jednotlivých zdrojů), • Přehled 10 nejčastějších bezpečnostních událostí za dané období agregovaných dle názvu a seřazených dle počtu výskytů, • Přehled bezpečnostních událostí pro 10 nejčastějších cílů (IP adres) za dané období, • Přehled bezpečnostních událostí pro 10 nejčastějších zdrojů (IP adres) za dané období, • Přehled 10 zdrojů (IP adres) za dané období s nejvyšším počtem odmítnutých odchozích spojení na firewallech, • Přehled 10 uživatelských účtů za dané období s nejvyšším počtem špatných přihlášení, • Přehled 10 uživatelských účtů za dané období s nejvyšším počtem úspěšných vzdálených přihlášení, • Popis relevantních bezpečnostních událostí s potenciálem přejít v kybernetické bezpečnostní incidenty s doporučením, jak je co nejlépe řešit, • Seznam a popis úprav pravidel a nastavení nástrojů, navržených na základě událostí, offenses a trendů za dané období. Jednotlivé typy bezpečnostních událostí jsou na základě vnitřního předpisu a dosavadní praxe rozděleny do 25 typů událostí zvaných podkategorie a 5 hlavních kategorií, určujících míru kritičnosti události v závislosti na tom, zda se jedná o významný nebo běžný informační systém – resp. zdroj dat.

<table>
<tr><th colspan="3">SERVICE LEVEL AGREEMENT (SLA)</th></tr>
<tr><td>Vyhodnocovací období</td><td colspan="2">1 kalendářní měsíc</td></tr>
<tr><td>SLA PARAMETRY</td><td>Jednotka</td><td>Hodnota</td></tr>
<tr><td>Dostupnost</td><td>[%/měsíc]</td><td>99</td></tr>
<tr><td>Provozní doba zaručená</td><td>[hod-hod]</td><td>0 - 24 (7x24)</td></tr>
<tr><td>Odstranění výpadku A1/A2</td><td>[hod v prac. době]</td><td>4h / 8h</td></tr>
<tr><td>Odstranění výpadku B3-B4</td><td>[dny]</td><td>NBD až 5 dnů</td></tr>
<tr><td>Odstranění výpadku C5</td><td>[dny]</td><td>10</td></tr>
<tr><th colspan="3">Způsob kontroly</th></tr>
<tr><td colspan="3">Do dostupnosti jsou počítány pouze incidenty typu A1 a A2, incidenty kategorie B3, B4 a C5 se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby bude prováděno 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 IP. Provozní činnosti budou kontrolovány Objednatelem (nebo jím stanoveným subjektem) na měsíční bázi.</td></tr>
<tr><th colspan="3">PODMÍNKY A OMEZENÍ SLUŽBY</th></tr>
<tr><td>Předpoklady služby</td><td colspan="2">Bezpečnostní monitoring bude zajišťován provozem nástrojů pro vyhodnocování bezpečnostních událostí na infrastruktuře Objednatele.
Objednatel pro účely poskytování služby zpřístupní bezpečnostní dohledové systémy (SIEM prostředí, včetně VPN přístupů) v potřebném rozsahu pro jejich správu.</td></tr>
<tr><td>Předpoklad personálního zajištění služby</td><td colspan="2">Zázemí Poskytovatele musí splňovat požadavky na minimální, certifikovaný řešitelský tým v obsazenosti 3 rolí, včetně požadavku na zastupitelnost a dostupnost reakce.
Jedná se minimálně o následující role:
L1 - dmin je role zajišťující implementaci, konfiguraci, aktualizace a upgrade, kontrolu a napojování zdrojů, správu HW, správu a nastavování licencí, řešení chyb v rámci implementovaného řešení, případná spolupráce s výrobcem řešení.
L2 - perátor zajišťující pravidelný monitoring se zaměřením na události dle kritičnosti, abnormality vybočující z normálu a dohled nad logováním zdrojů se zaměřením na možné výpadky a absenci dat.
L3 - analytik je role zajišťující podrobnou analýzu událostí a převod do kategorie “incident”, včetně reportingu. Řeší následnou optimalizaci a nastavování bezpečnostních pravidel, vytváření pravidel na míru prostředí, vytváření nových pravidel dle aktuálních hrozeb, řádný reporting, reporting mimořádných událostí, konzultace k bezpečnostním událostem, školení o používání nástroje SIEM a další.</td></tr>
</table>

Výjimky služby	Odstávky způsobené nedostupností monitorovaných zařízení či jiných infrastrukturních součástí, které jsou mimo odpovědnost Poskytovatele, jsou vyloučeny ze SLA. V případě, kdy prokazatelně došlo k výpadku služby v přímém důsledku neodborné činnosti provedené zástupci Objednatele, tak je Poskytovatel zproštěn veškerých negativní důsledků vyplývajících z takového výpadku, včetně vyloučení výpočtu SLA u těchto zařízení.

KL03 – POSKYTOVÁNÍ AD-HOC SLUŽEB SPECIALISTŮ

POPIS SLUŽBY

Poskytování služeb a rozšířeného poradenství v oblasti kyberbezpečnosti

Služby specialistů specifikují obecné typy činnosti, jenž může Poskytovatel vykonávat a budou objednávány nad rámec paušální platby za KL 1-2.

Služby specialistů, tak mohou zahrnovat:

- řešení událostí a incidentů nad limitaci uvedenou v KL,
- kontrolu, převzetí a zařazení nových významných zdrojů událostí do Platformy SIEM,
- konfigurační práce při významné novelizaci požadavků kybernetické bezpečnosti či Objednatele ve vztahu k SIEM,
- školení a tvorbu metodické podpory provozu a rozvoje SIEM,
- integrace nových systémů poskytující či konzumující služby pro/ze SIEM,
- rozvoj samotné Platformy SIEM např. při rozšíření licencí či modulů,
- podpora konzultanta produktu SIEM při jednáních se třetí stranou,
- vývoj integračních můstků, parserů či dalších Use-Case Platformy SIEM, jedná se typicky o činnosti:
    - vývojové a testovací,
    - rozvoj reportů včetně druhů reportů,
    - konzultační a dokumentační činnosti.
- Tyto služby mohou zahrnovat i netechnickou, tj. metodickou podporu:
    - tvorbu a údržbu nadstandartní Dokumentace SIEM,
    - konzultační činnosti napojení SIEM na ostatní systémy provozu a bezpečnosti
    - spolupráci při návrhu IS architektury a integrací do SIEM,
    - tvorbu metodiky a způsobu poskytování Platformy SIEM,
    - konzultace a řešení spojené se zavedením ostatních norem bezpečnosti
- metodická podpora implementace nápravných opatření zjištěných pomocí SIEM

PARAMETRY SLUŽBY

1. Měrná jednotka:
    - člověkoden
2. Limit objemu služby:
    - dle dílčích objednávek
    - do vyčerpání limitu smlouvy

3. Doba provozu služby:

- 8x5x365

ZPŮSOB ČERPÁNÍ SLUŽBY

Služby budou hrazeny na základě ceny Služeb specialistů v následujících rolích:

- Projektový manažer,
- Specialista architekt řešení,
- Specialista řízení IT služeb,
- Specialista systémů řízení bezpečnosti informací (SŘBI),
- IT specialista SIEM
- Bezpečnostní analytik SIEM,
- IT specialista ochrany databází,
- IT specialista správy zranitelností,
- IT specialista OS Linux,
- IT specialista OS Windows,

C) Služby exitu

Případné poskytnutí Služeb exitu spojených se závěrečným ukončením poskytování Služeb spočívá v přípravě a předání Platformy SIEM novému poskytovateli na konci smluvního vztahu vč. jeho předčasného ukončení podle pokynů objednatele, které zahrnují zejména:

- poskytnutí potřebné součinnosti podle pokynů objednatele novému poskytovateli,
- předání veškeré dokumentace a potřebných informací,
- řádné předání všech potřebných dat včetně dat doplňkových,
- vypracování Exitového plánu v dostatečném předstihu a poskytnutí nezbytné součinnosti k jeho realizaci.

D) SLA (úroveň poskytování služeb)

V případech, kdy Poskytovatel v rámci poskytování Služeb (*Service level Agreement, SLA*), jejichž předmět je smluvně vymezen příslušným Katalogovým listem, nedosáhne stanovené (dohodnuté) úrovně plnění, vzniká tímto objednateli nárok na jednorázovou slevu z ceny za Služby. Za nedosažení stanovené (dohodnuté) úrovně plnění se nepočítá doba plánované odstávky Platformy SIEM anebo dané Odstávky služby. Výše jednorázové slevy bude stanovena dle příslušného SLA parametru, který byl porušen a dle úrovně porušení (specifikovaná jednotlivě pro každý SLA parametr). V případě, že v důsledku výpadku jedné Služby dojde k výpadku i dalších Služeb, platí, že sleva z ceny se uplatní pouze pro danou Službu, která způsobila výpadek i ostatních Služeb. V případě, že dojde k nedodržení více dílčích SLA parametrů v rámci jedné Služby, platí, že sleva z ceny se uplatní ke všem nedodrženým dílčím SLA parametrům.

Definice SLA pro jednotlivé katalogové listy

a) Dostupnost

Dostupností je míněna dostupnost Platformy SIEM a poskytované Služby dle Smlouvy, v průběhu Provozní doby zaručené, vyhodnocovaná v rámci Vyhodnocovacího období. Na dostupnost, resp.

nedostupnost Služby mají dopad incidenty kategorie A (incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují). Dostupnost Služby je vyhodnocována v procentech za Vyhodnocovací období.

b) Provozní doba zaručená
Provozní dobou zaručenou je míněna provozní doba Služby, v průběhu, které je Objednatelem požadovaná a současně Poskytovatelem garantovaná plná Dostupnost Služby, a to včetně podpory ze strany **Poskytovatele**. Provozní doba zaručená je měřena/vyhodnocována v jednotkách času (v hodinách). Dostupnost Služby, resp. úroveň/rozsah její Dostupnosti v době mimo Provozní dobu zaručenou je specifikována příslušném katalogovém listě.

c) Maximální doba výpadku
Maximální dobou výpadku je míněno maximální časové období, po které je v rámci Provozní doby zaručené přípustná jednorázová nedostupnost Služby. Maximální doba výpadku je vyhodnocována v jednotkách času (v hodinách).

d) Maximální doba nedostupnosti dat
Maximální dobou nedostupnosti dat je míněna ztráta nebo nedostupnost transakčních, aplikačních či systémových dat využívaných/spravovaných danou Službou, vyhodnocovaná v rámci Vyhodnocovacího období. Maximální doba nedostupnosti dat je vyhodnocována v jednotkách času (v hodinách).

e) Maximální doba zahájení řešení incidentu/požadavku
Maximální dobou zahájení řešení incidentu/požadavku je míněna doba, do které je Poskytovatel povinen zareagovat na nový záznam v helpdeskovém systému, který byl založen v rámci Provozní doby zaručené. Maximální doba zahájení řešení incidentu/požadavku je vyhodnocována v jednotkách času (v minutách).

Odstranění výpadku – Priority: A, B a C
Jednotlivé kategorie incidentů jsou uvedeny v příslušných katalogových listech. Odstranění výpadku je měřeno/vyhodnocováno v jednotkách času (v hodinách pro kategorii A, ve dnech pro kategorie B a C). Čas potřebný k odstranění hardwarové závady třetí smluvní stranou (např. servis třetích stran, jakožto přímým smluvním partnerem Objednatele), se do doby Odstranění výpadku nezapočítává. Plánované odstávky Infrastruktury anebo dané Služby se do doby výpadku nezapočítávají.

Priorita	**Definice priority požadavku**
Kategorie A1 **Kritická**	Některé nebo všechny části poskytovaných Služeb selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Platformy SIEM.
Kategorie A2 **Vysoká**	Poskytované Služby jsou podstatně omezeny, některé části selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je zásadním způsobem ovlivněna činnost Platformy SIEM.
Kategorie B3 **Střední**	Služby jsou funkční pouze částečně, Služby jsou ovlivněny selháním nebo omezením některé ze systémových funkcí podporujících důležité činnosti Služeb. Některá ze služeb z vnějšího rozhraní vykazuje funkční vady, pouze některé funkce pro jednotlivé části Platformy SIEM nejsou plně funkční.
Kategorie B4 **Nízká**	Integrační platforma je operativní, závada nemá vliv na činnost Platformy SIEM. Vyskytují se nedostatky nepodstatné povahy, které způsobují například

Priorita	Definice priority požadavku
	nekomfortní ovládání uživatelem ztěžující běžný provoz, resp. zvyšující pracnost činností v běžném provozu. Priorita požadavku zároveň zahrnuje situace, kdy některé funkce prokazatelně selhaly, ale nejsou v daný moment využívány nebo nemají žádný vliv na řádný chod Platformy SIEM.
Kategorie C5 **Ostatní**	Požadavkem je žádost o podání informace (dotaz, vysvětlení). Priorita požadavku zároveň zahrnuje situace, kdy některé funkce prokazatelně selhaly, ale nejsou v daný moment využívány nebo nemají žádný vliv na řádný chod Platformy SIEM.

Níže uvedená tabulka zobrazuje výčet parametrů SLA s příslušnými slevami z příslušné ceny za poskytování Služeb dle smlouvy a způsobem výpočtu.

Název parametru	Výše slevy z ceny příslušné ceny Služby v Kč (bez DPH) za každý jednotlivý případ vzniku nároku na slevu	Způsob výpočtu
Dostupnost Služby	500,-	Za každou započatou 1 hodinu nedostupnosti Služby dle katalogového listu nad požadovanou Dostupnost Služby dle Katalogové listu
Max. doba výpadku	400,-	Za každou započatou 1 hodinu výpadku Služby dle Katalogového listu nad Maximální dobu výpadku Služby dle Katalogového listu
Max. doba nedostupnosti dat	400,-	Za každou započatou 1 hodinu nedostupnosti dat nad stanovenou Maximální dobu nedostupnosti dat dle Katalogového listu
Doba odezvy kategorie A2	100,-	Za každou započatou hodinu nad stanovenou Dobu odezvy kategorie A2 definovanou výše
Odstranění výpadku kategorie A1	400,-	Za každou započatou 1 hodinu nad stanovenou dobu pro Odstranění výpadku kategorie A1 definovanou výše
Odstranění výpadku kategorie A2	300,-	Za každou započatou 1 hodinu nad stanovenou dobu pro Odstranění výpadku kategorie A2 definovanou výše
Odstranění výpadku kategorie B3	250,-	Za každý započatý den nad stanovenou dobu pro Odstranění výpadku kategorie B2 definovanou výše
Odstranění výpadku kategorie B4	200,-	Za každý započatý den nad stanovenou dobu pro Odstranění výpadku kategorie B4 definovanou výše
Odstranění výpadku kategorie C5	100,-	Za každý započatý den nad stanovenou dobu pro Odstranění výpadku kategorie C5 definovanou výše

E) Harmonogram Dodávek a plnění Služeb

T = datum uveřejnění smlouvy v registru smluv

	Předmět plnění	Termín zahájení plnění	Max.Termín ukončení plnění
Jednorázové dodávky a služby	Vypracování projektu Detailního návrhu řešení migrace stávajícího SIEM řešení do nového prostředí SIEM – Služby převzetí	T	T + 20 kalendářních dnů
	Dodávka SIEM a instalace řešení SIEM a zahájení podpory (včetně dodávky 48 měsíců předplacené software podpory výrobce řešení)	T	T + 20 kalendářních dnů
	Migraci stávajícího řešení a politik SIEM a zpracování implementační dokumentace nasazení SIEM	T	T + 30 kalendářních dnů
Kontinuální služby	KL-01 - Správa platformy SIEM	T + 1 měsíc	T1 + 48 měsíců
	KL-02 - Služby bezpečnostního monitoringu	T + 1 měsíc	T1 + 48 měsíců
	KL-03 – Poskytování ad-hoc Služeb specialistů	T + 1 měsíc	T1 + 48 měsíců
	Poskytnutí programového vybavení formou SaaS	T + 1 měsíc	T1 + 48 měsíců
Služby exitu	Služby EXITU (budou-li objednány)	T + 48 měsíců	T48 + 1 měsíc

Seznam členů realizačního týmu

Seznam členů realizačního týmu, kteří se budou podílet na plnění veřejné zakázky, včetně doložení příslušné odbornosti:

Název pozice	Jméno a příjmení člena týmu	Požadavky	Způsob splnění kritéria kvalifikace (prokázání)
Projektový manažer	Ing. Tomáš Myslivec Zaměstnanec dodavatele	Ukončené vysokoškolské vzdělání.	Dodavatel prokazuje předložením kopie vysokoškolského diplomu.
		Platná certifikace v oblasti projektového řízení na úrovni Prince 2 – Practitioner certificate in Project management nebo vyšší nebo certifikace IMPA D nebo PMI CAPM. K prokázání požadavků zadavatele postačí předložit alespoň jednu z výše uvedených certifikací.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.
Specialista architekt řešení	Ing. Ondřej Salák Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Ukončené vysokoškolské vzdělání.	Dodavatel prokazuje předložením kopie vysokoškolského diplomu.
		Platná certifikace v oblasti návrhu a architektury informačních technologiína úrovni: TOGAF 9 Foundation nebo vyšší. Zadavatel umožňuje předložit i obdobné certifikace např. Archimate Foundation, IASA Associate či CITA-P (Certified lnformation Technology Architect Professional Certification). K prokázání požadavků zadavatele postačí předložit alespoň jednu z výše uvedených certifikací.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.

Specialista řízení IT služeb	Antonín Šefčík Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Ukončené vysokoškolské vzdělání.	Dodavatel prokazuje předložením kopie vysokoškolského diplomu.
		Platná certifikace v oblasti řízení a správy IT služeb na úrovni: ITIL – Foundation nebo vyšší. Zadavatel umožňuje předložit i obdobné certifikace např. Lead auditor pro IT služby. K prokázání požadavků zadavatele postačí předložit alespoň jednu z výše uvedených certifikací.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.
Specialista systémů řízení bezpečnosti informací (SŘBI)	Ing. Stanislav Kollert Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace v oblasti řízení bezpečnosti informací na úrovni: Information Security Management System Lead Auditor (ISO/IEC 27001) nebo CISA (Certified Information Systems Auditor) nebo CISSP (Certified Information Systems Security Professional). K prokázání požadavků zadavatele postačí předložit alespoň jednu z výše uvedených certifikací.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.
IT specialista SIEM #1	Martin Hansgut Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace specialisty na řešení IBM SIEM na úrovni: i. IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2 nebo vyšší a zároveň ii. IBM Certified Deployment Professional - IBM QRadar SIEM V7.3.2 nebo vyšší. K prokázání požadavků zadavatele je nutno	Dodavatel prokazuje předložením kopií požadovaných certifikátů.

		předložit obě výše uvedené certifikace.	
IT specialista SIEM #2	Josef Hradečný Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace specialisty na řešení IBM SIEM na úrovni: i. IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2 nebo vyšší a zároveň ii. IBM Certified Deployment Professional - IBM QRadar SIEM V7.3.2 nebo vyšší.. K prokázání požadavků zadavatele je nutno předložit obě výše uvedené certifikace.	Dodavatel prokazuje předložením kopií požadovaných certifikátů.
Bezpečnostní analytik SIEM #1	Jan Novák Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace analytika na řešení IBM SIEM na úrovni: i. IBM Certified Associate Analyst - IBM QRadar SIEM V7.3.2 nebo vyšší a zároveň ii. IBM Certified Deployment Professional - IBM QRadar SIEM V7.3.2 nebo vyšší. K prokázání požadavků zadavatele je nutno předložit obě výše uvedené certifikace.	Dodavatel prokazuje předložením kopií požadovaných certifikátů.
Bezpečnostní analytik SIEM #2	David Hálek Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace analytika na řešení IBM SIEM na úrovni: i. IBM Certified Associate Analyst - IBM QRadar SIEM V7.3.2 nebo vyšší a zároveň ii. IBM Certified Deployment Professional - IBM QRadar SIEM V7.3.2 nebo vyšší. K prokázání požadavků zadavatele je nutno předložit obě výše uvedené certifikace.	Dodavatel prokazuje předložením kopií požadovaných certifikátů.

IT specialista ochrany databází	Radim Navrátil Zaměstnanec Zaměstnanec poddodavatele Next Generation Security Solutions s.r.o.	Platná certifikace pro řešení ochrany databázového prostředí IBM Guardium a IBM Qradar na úrovni: i. IBM Certified Administrator Security Guardium V10.0 nebo vyšší a zároveň ii. IBM Certified Associate Administrator Security Guardium Data Protection V10.1.2 nebo vyšší a zároveň iii. IBM Certified Associate Analyst - IBM QRadar SIEM V7.3.2 nebo vyšší. K prokázání požadavků zadavatele je nutno předložit všechny tří výše uvedené certifikace.	Dodavatel prokazuje předložením kopií požadovaných certifikátů.
IT specialista správy zranitelností	Jan Kučera Zaměstnanec dodavatele	Platná certifikace od výrobce nabízeného řešení IBM pro správu bezpečnostních incidentů SIEM nebo certifikace CompTIA Security+ či Ethical hacker (CEH). K prokázání požadavků zadavatele postačí předložit alespoň jednu z výše uvedených certifikací.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.
IT specialista OS Linux	Tomáš Horáček Zaměstnanec dodavatele	Platná certifikace (RHCE) na úrovni Redhat Enterprise Linux Certified Engineer v.8 nebo vyšší. Zadavatel pro vyloučení pochybností uvádí, že se jedná o jedinou certifikaci.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.
IT specialista OS Windows	Jiří Veličkov Zaměstnanec dodavatele	Platná certifikace MCSA nebo MCSE v oblasti serverů Microsoft.	Dodavatel prokazuje předložením kopie požadovaného certifikátu.

Příloha č. 3 smlouvy - Oceněný kalkulační model

ID	Dílčí plnění	Množství	Cena za jednotku Množství v Kč bez DPH	Cena celkem v Kč bez DPH
1	Služby převzetí Zpracování implementační dokumentace nasazení SIEM Migrace dat ze stávajícího řešení nástroje pro zavedení SIEM	1	150 000,00 Kč	150 000,00 Kč
2	Dodávka licencí výrobce pro platformu SIEM (SW), včetně subscripce na 48 měsíců	1	10 950 000,00 Kč	10 950 000,00 Kč
3	Dodávka licencí výrobce pro platformu SIEM (SW), včetně subscripce na 12 měsíců	1	2 200 000,00 Kč	2 200 000,00 Kč
4	Paušál za 1 kalendářní měsíc KL - 01 - Správa platformy SIEM	48	32 000,00 Kč	1 536 000,00 Kč
5	Paušál za 1 kalendářní měsíc KL - 02 - Služby bezpečnostního monitoringu	48	120 000,00 Kč	5 760 000,00 Kč
6	Cena za 1 člověkoden poskytování ad-hoc služeb specialistů KL - 03	300	12 800,00 Kč	3 840 000,00 Kč
7	Služby EXITu	1	150 000,00 Kč	150 000,00 Kč
8	Cena za 1 člověkoden služeb správy a bezpečnostního monitoringu SIEM / SOC nad rámec KL 01-02	90	12 000,00 Kč	1 080 000,00 Kč
				25 666 000,00 Kč