SMLOUVA O DÍLO

podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Smluvní strany

město Sokolov

se sídlem Rokycanova 1929, 356 01 Sokolov,

IČ: 00259586, DIČ: CZ00259586,

zastoupené: Renatou Oulehlovou, starostkou,

bankovní spojení: [redacted]

(dále jako „**Objednatel**")

a

IXPERTA s.r.o.

se sídlem Lihovarská 1060/12, 190 00 Praha 9

zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze pod sp. zn. C 117991

IČ:27599523 DIČ: CZ27599523

zastoupená Pavlem Šiprem

bankovní spojení [redacted]

(dále jako „**Zhotovitel**")

(výše uvedené smluvní strany se dále označují jednotlivě též jen jako „smluvní strana", nebo společně též jen jako „smluvní strany)

uzavřely níže uvedeného dne, měsíce a roku podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, (dále jen „Občanský zákoník") tuto smlouvu o dílo.

1 Předmět smlouvy

1.1 Předmětem této smlouvy je Implementace upgrade systému monitorování bezpečnostních incidentů a událostí (dále také jen „SIEM") v síti provozované objednatelem v jeho sídle.

1.2 Zhotovitel se zavazuje, že v rámci implementace podle odst. 1.1 provede následující úkony:

a) zpracování předimplementační analýzy,
b) dodávka SIEM řešení, vč. předplacené podpory výrobce na 4 roky,
c) dodání veškeré potřebné implementační dokumentace vztahující se k dílu podle této smlouvy,
d) proškolení uživatelů (správce),
a to v rozsahu a za podmínek podle přílohy č. 1 k této smlouvě.

1.3 Zhotovitel se dále zavazuje poskytovat Objednateli rozšířenou podporu SIMEM po dobu 4 let, a to v rozsahu a za podmínek podle přílohy č. 1 k této smlouvě, která bude specifikována v samostatné smlouvě o provádění technického servisu systému monitorování bezpečnostních incidentů a událostí (SIEM) v síti.

1.4 Objednatel se zavazuje, že

a) vytvoří podmínky pro to, aby Zhotovitel mohl dílo v rozsahu dle ustanovení bodu 1.2 této smlouvy řádně a včas provést a

b) za řádně provedené dílo zaplatí Zhotoviteli sjednanou cenu dle příslušných ustanovení této smlouvy.

2 Technická specifikace díla

2.1 Technická specifikace díla podle čl. 1 je uvedena v Příloze č. 1, jež je nedílnou součástí této smlouvy.

3 Časové údaje o provádění díla

3.1 Zhotovitel se zavazuje provádět dílo v rozsahu bodu 1.2 této smlouvy dle časového harmonogramu uvedeného v Příloze č. 2, jež je nedílnou součástí této smlouvy.

3.2 Plnění ze strany Zhotovitele je podmíněno řádnou a včasnou součinností, která je specifikovaná v Příloze č. 3 dle této smlouvy. Po dobu prodlení Objednatele s poskytnutím součinnosti není Zhotovitel v prodlení se svým plněním.

3.3 Dnem zdanitelného plnění Zhotovitele je den skutečného předání/převzetí díla příslušnými zástupci smluvních stran.

3.4. Termín dodání díla je max. do 2 měsíců od účinnosti této smlouvy.

3.5. Místo plnění díla je sídlo objednatele.

4 Cena, platební podmínky

4.1 Objednatel zaplatí Zhotoviteli za provedení díla v rozsahu čl. 1 odst. 1.2 a za poskytování rozšířené podpory podle čl. 1 odst. 1.3 této smlouvy celkovou cenu ve výši **569 242** Kč (slovy: pět set šedesát devět tisíc dvě stě čtyřicet dva korun českých) bez DPH a **688 783** Kč (slovy: šest set osmdesát osm tisíc sedm set osmdesát tři korun českých včetně DPH. Celková cena sestává z ceny za dílo podle čl. 1 odst. 1.2 ve výši **371 062** Kč (slovy: tři sta sedmdesát jedna tisíc šedesát dva korun českých) bez DPH a z ceny za poskytování rozšířené podpory podle čl. 1 odst. 1.3 ve výši Kč **198 180** (slovy: jedno sto devadesát osm tisíc jedno sto osmdesát korun českých) bez DPH. Položkový rozpočet je uveden v Příloze č. 5 této smlouvy.

4.2 Úhrada ceny bude prováděna na základě předloženého a odsouhlaseného (zástupcem Objednatele) plnění (dodací list). Ke všem cenám účtuje Zhotovitel navíc DPH podle předpisů platných ke dni uskutečnění příslušného zdanitelného plnění. Cena za poskytování rozšířené podpory podle čl. 1 odst. 1.3 se hradí měsíčně pozadu.

4.3 Objednatel uhradí Zhotoviteli cenu díla na základě faktury, která bude obsahovat (splňovat) náležitosti ve smyslu příslušných ustanovení zákona, zejména též podstatné údaje o předmětu plnění.

4.4 V případě, že faktura nebude obsahovat náležitosti uvedené v této smlouvě, je Objednatel oprávněn vrátit ji Zhotoviteli k doplnění/opravě. V takovém případě se přeruší plynutí lhůty splatnosti a nová lhůta splatnosti začne plynout doručením opravené faktury Objednateli.

4.5 Lhůta splatnosti faktur je 14 kalendářních dnů od doručení – převzetí faktury Objednatelem, přičemž Zhotovitel je oprávněn fakturu vystavit až po předání a převzetí díla podle čl. 6 odst. 6.4, vyjma faktury na zaplacení ceny za poskytování rozšířené podpory, kterou je zhotovitel oprávněn vystavit nejdříve v měsíci následujícím po měsíci, v němž byla rozšířená podpora poskytnuta.

4.6 Faktura (daňový doklad) s výše uvedenými náležitostmi se doručuje na adresu Objednatele uvedenou v záhlaví smlouvy.

4.7 Cena za dílo uvedená v tomto článku je konečná, nejvýše přípustná a pevná a zahrnuje veškeré náklady Zhotovitele související s plněním předmětu smlouvy, vč. nákladů na dopravu. Jediným důvodem změny výše ceny je změna zákonné sazby DPH. Objednatel neposkytuje jakékoli zálohy.

5 Provádění díla

5.1 Zhotovitel prohlašuje, že se seznámil se všemi podklady, které určují předmět smlouvy, a že splňuje veškeré podmínky a požadavky podle této smlouvy, je dostatečně odborně způsobilý k plnění jejího předmětu, tj. je odborníkem ve smyslu § 2950 občanského zákoníku, pokud jde o předmět smlouvy, a je oprávněn ji uzavřít a řádně plnit závazky v ní obsažené a k okamžiku uzavření této smlouvy nebyl na jeho majetek prohlášen konkurs, nedošlo k jeho zamítnutí pro nedostatek majetku ani k zamítnutí insolvenčního návrhu proto, že jeho majetek nepostačoval k úhradě nákladů insolvenčního řízení, není v likvidaci a nemá daňové nedoplatky na území České republiky ani v zemi sídla nebo místa podnikání či bydliště.

5.2 Zhotovitel se zavazuje provádět dílo ve stanoveném rozsahu a ve stanovených časových lhůtách. V případě potřeby součinnosti Objednatele vyzve Zhotovitel Objednatele min. pět (5) dní předem.

5.3 Zhotovitel se zavazuje při provádění díla postupovat s odbornou péčí. Svoji činnost bude přitom vykonávat v souladu se zájmy Objednatele a podle jeho pokynů.

5.4 Objednatel je oprávněn kdykoliv kontrolovat či nechat kontrolovat provádění díla. Zhotovitel se zavazuje umožnit Objednateli přístup na místo plnění, resp. na pracoviště, kde se plnění provádí, i do přilehlých prostor a poskytnout mu při tom potřebnou součinnost.

5.5 Zjistí-li Objednatel, že Zhotovitel provádí dílo v rozporu se svými závazky dle této smlouvy nebo v rozporu se zákonem, je oprávněn dožadovat se toho, aby Zhotovitel neprodleně odstranil závadný stav a dílo prováděl řádně.

Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.

5.6 Smluvní strany se dohodly ustanovit/jmenovat své zástupce, kteří jsou oprávněni jednat jménem smluvních stran v technickoprovozních a obchodních záležitostech souvisejících s plněním této smlouvy. Seznamy zástupců jsou uvedeny v Příloze č. 4, jež je nedílnou součástí této smlouvy.

6 Předání a převzetí díla

6.1 Předání a převzetí díla proběhne na základě akceptačních testů, které porovnají skutečné vlastnosti díla se specifikací díla uvedenou v Příloze č. 1. Akceptační testy budou připraveny při realizaci díla jako část předimplementační analýzy Zhotovitele.

6.2 Zhotovitel bude písemně informovat Objednatele nejméně sedm (7) dní předem o termínu zahájení akceptačních testů. Objednatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání.

6.3 Jestliže dílo splní akceptační kritéria akceptačních testů, má se za to, že bylo řádně předáno a Objednatelem převzato, o čemž strany pořídí protokol.

6.4 Jestliže dílo nesplňuje stanovená akceptační kritéria kteréhokoliv akceptačního testu, je Objednatel oprávněn odmítnout dílo převzít; v takovém případě se o odmítnutí převzetí pořídí zápis, ve kterém se uvedou a popíší veškeré zjištěné nedostatky. Zhotovitel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu. Dílo se považuje za předané a převzaté v okamžiku, kdy nebude vykovat vady či nedodělky a bude splňovat veškerá akceptační kritéria podle odst. 6.3.

7 Odpovědnost za vady a škody

7.1 Odpovědnost Zhotovitele za vady díla a za škody se řídí příslušnými ustanoveními Občanského zákoníku.

7.2 Zhotovitel odpovídá jen za škodu, jež vznikla zaviněným porušením jeho právních povinností nebo právně relevantní škodní událostí, k níž je jeho odpovědnost přímo stanovena zákonem.

8 Vyšší moc

8.1 Smluvní strany se osvobozují od odpovědnosti za částečné nebo úplné nesplnění smluvních závazků v případě, že se tak stalo v důsledku smluvními stranami nezaviněných, mimořádných, nepředvídatelných a neodvratitelných událostí, majících vliv na plnění předmětu této smlouvy (dále jen „vyšší moc"). Za vyšší moc jsou považovány zejména tyto skutečnosti:

- přírodní katastrofy (včetně nepředvídatelných, neobvyklých podmínek počasí, jestliže jejich působení nebude možno čelit),
- válka, revoluce, sabotáž a skutečnosti válce podobné,
- stávky mající legální charakter.

8.2 Smluvní strany se dohodly, že smluvní pokuty nebudou v případě prodlení z důvodu vyšší moci uplatňovány.

8.3 V případě, že Zhotovitel nebude schopen dodržet termíny stanovené v této smlouvě z důvodů vyšší moci, budou stanoveny nové termíny, které budou splnitelné s ohledem na vzniklé okolnosti.

9 Důvěrné informace

9.1 Smluvní strany jsou si vědomy toho, že v rámci plnění této smlouvy:

a) si mohou vzájemně úmyslně nebo i opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen "důvěrné informace"),

b) mohou vědomou činností druhé strany nebo i jejím opomenutím získat přístup k důvěrným informacím druhé strany.

9.2 Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství ve smyslu ustanovení § 504 Občanského zákoníku, tj. například, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.

9.3 Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přejímající strana vyvine pro zachování jejich důvěrnosti stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou případů, kdy to bude nezbytné pro plnění této smlouvy, se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této smlouvy nebo objednávek.

9.4 Pokud jsou důvěrné informace aktivně poskytovány v písemné podobě anebo ve formě datových souborů na počítačových médiích, je předávající strana povinna upozornit přejímající stranu na

důvěrnost takového materiálu jejím přiměřeným označením.

9.5 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

a) se staly veřejně známými, aniž by to zavinila záměrně či opominutím přejímající strana,

b) měla přejímající strana legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,

c) jsou výsledkem postupu, při kterém k nim přejímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo informacemi třetí strany, bez ohledu na to, zda obsahuje důvěrné informace či nikoli.

9.6 Účinnost ustanovení o ochraně informací uvedených výše není dotčena ukončením účinnosti této smlouvy z jakéhokoliv důvodu a trvá ještě dva roky po ukončení účinnosti této smlouvy.

9.7 Ujednáními tohoto článku nejsou dotčeny povinnosti stanovené Objednateli obecně závazným právním předpisem, zejména zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a 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. Poskytnutí informací vč. poskytnutí kopie této smlouvy vč. jejích příloh nebo uveřejnění této smlouvy prostřednictvím registru smluv není porušením povinností podle této smlouvy.

10 Smluvní pokuty

10.1 Smluvní strany se dohodly, že Objednatel může uplatnit nárok na smluvní pokutu vůči Zhotoviteli v následujících případech a výši:

a) prodlení s termínem předání díla ve výši 1 000 Kč za každý den prodlení,

b) prodlení s odstraňováním vad či nedodělků zjištěných při ve výši 1 000 Kč za vadu či nedodělek a den prodlení,

c) porušení jakékoliv jiné povinnosti uvedené v této smlouvě ve výši 500 Kč za každý den prodlení s nápravou přes výzvu či upozornění Objednatele o více než 3 dny po obdržení takovéto výzvy.

10.2 Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody převyšující smluvní pokutu, ani na odstoupení od této smlouvy jakož ani povinnost Zhotovitele splnit jeho závazek podle této smlouvy.

10.3 Smluvní pokuta je splatná na základě písemné výzvy Objednatele do 15 dnů od doručení výzvy Zhotoviteli převodem na účet uvedený v záhlaví této smlouvy.

10.4 Zhotovitel považuje smluvní pokuty sjednané v tomto článku za přiměřené a vzdává se práva domáhat se u soudu jejich snížení.

11 Odstoupení

11.1 Objednatel je kromě důvodů pro odstoupení od smlouvy stanovených občanským zákoníkem oprávněn odstoupit od této smlouvy v případě, že:

a) zhotovitel je v prodlení s dokončením díla či jeho části oproti termínu podle čl. 3 odst. 3.4 déle než 20 dnů,
b) Zhotovitele je v prodlení s prováděním díla o více než 20 dnů oproti v harmonogramu podle přílohy č. 2 k této smlouvě,
c) neodstraní-li Zhotovitel vadu díla či jeho části včas nebo vadu odmítne odstranit,
d) Zhotovitel soustavně nebo zvlášť hrubým způsobem poruší podmínky jakosti díla,
e) proti Zhotoviteli bude zahájeno insolvenční řízení a insolvenční návrh nebude v zákonné lhůtě odmítnut pro zjevnou bezdůvodnost nebo insolvenční návrh prodávajícího bude

zamítnut proto, že majetek prodávajícího nepostačuje ani k úhradě nákladů insolvenčního řízení, anebo prodávající vstoupí do likvidace.

11.2 Zhotovitel je oprávněn odstoupit od smlouvy v případě, že Objednatel je v prodlení s úhradou ceny díla déle než 30 dní.

11.3 Účinky odstoupení nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

11.4 Odstoupením od smlouvy není dotčen nárok na smluvní pokutu.

12 Závěrečná ustanovení

12.1 Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv podle 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. Smluvní strany se dohodly, že smlouvu zašle správci registru smluv k uveřejnění podle předchozí věty Objednatel.

12.2 Účinnost této smlouvy lze předčasně ukončit písemnou dohodou smluvních stran.

12.3 Kterákoliv smluvní strana může od této smlouvy odstoupit podle ustanovení § 2001 a násl. občanského zákoníku, zejména v případě podstatného porušení smluvních závazků z této smlouvy druhou ze smluvních stran. Za podstatné porušení povinností se považuje zejména:

A) nedodržení a nesplnění podmínek dodání díla dle odstavce č. 1.2 a 1.3 této smlouvy,

B) nedodržení a nesplnění termínu dodání díla dle odstavce 3.4 této smlouvy.

Účinky odstoupení od smlouvy nastávají dnem doručení oznámení o odstoupení druhé smluvní straně.

Při odstoupení od této smlouvy jsou smluvní strany povinny provést vzájemné vypořádání ve lhůtě do 30 (třiceti) od účinků odstoupení.

12.4 Jakákoliv případná předběžná ujednání v souvislosti s předmětem této smlouvy pozbývají platnosti a smluvní vztahy se napříště budou řídit jen touto smlouvou.

12.5 Jakékoliv změny a doplnění této smlouvy mohou být provedeny jen písemnou formou postupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran.

12.6 Stane-li se některé z ustanovení této smlouvy neplatným nebo neúčinným, platnost a účinnost ostatních ustanovení tím není dotčena. Neplatné nebo neúčinné ustanovení bude nahrazeno jiným ustanovením platným a účinným, které co nejblíže odpovídá původnímu smyslu a účelu neplatného nebo neúčinného ustanovení.

12.7 Pokud nastanou mezi smluvními stranami jakékoli spory v souvislosti s touto smlouvou, budou je smluvní strany řešit přednostně smírčím postupem na úrovni svých statutárních zástupců.

Spory, které nebudou urovnány tímto smírčím postupem smluvních stran, budou s konečnou platností rozhodovány příslušným soudem podle místa sídla Objednatele.

12.8 Tato smlouva je vyhotovena ve dvou vyhotoveních s platností originálu, z nichž každá ze smluvních stran obdrží po jednom vyhotovení.

12.9 Obě smluvní strany prohlašují, že tato smlouva byla sepsána podle jejich pravé a svobodné vůle, nikoliv v tísni nebo za jinak jednostranně nevýhodných podmínek, že si ji řádně přečetly, souhlasí s ní a na důkaz závaznosti a souhlasu ji podepisují.

12.10 O uzavření této smlouvy rozhodla Rada města Sokolova dne 23.01.2019 usnesením č. 76/3RM/2019.

12.11 Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1: Technická specifikace díla

Příloha č. 2: Časový harmonogram realizace díla

Příloha č. 3: Specifikace součinnosti ze strany Objednatele

Příloha č. 4: Seznam zástupců

Příloha č. 5: Položkový rozpočet – vlastní cenová nabídka zhotovitele

V Praze dne 29.1.2019

V Sokolově dne: 31.1.2019

Za Zhotovitele:

[redacted]

Pavel Šipr, jednatel společnosti

Za Objednatele:

[redacted]

Renata Oulehlová, starostka města

IXPERTA

IXPERTA s. r. o.
Lihovarská 1060/12
190 00 Praha 9
IČ: 27599523
DIČ: CZ27599523

Příloha č. 1 - Technická specifikace díla:

1. Obsah specifikace projektu:

2. ANALÝZA A PROJEKT:

- Zadavatel požaduje zpracovat předimplementační analýzu (pro upgrade produktu Extreme SIEM V7.2 od Extreme Networks na QRADAR SIEM V7.3 od IBM), která musí popsat a konkretizovat implementaci řešení, dle požadavků zadání. Formát dokumentu Microsoft DOC.
- Celý dokument Analýza a projekt bude vyhodnocen v oponentuře Zadavatele, až po zapracování připomínek bude schválen, následně může být přistoupeno k implementaci upgrade.

Obsahem analýzy musí být minimálně:

2.1. Technický návrh řešení:

Identifikovat (ovčřit) všechny zdroje logů, minimálně bude popsáno:

- Označení, kategorizace a popis zdrojů logů
- Stanovení metod sběru logů
- Zjištění míst ukládaných logů IS
- Stanovení míry zabezpečení přenášené komunikace (posílání a vyčítání logů)
- Ohodnocení důležitosti zdrojů logů
- Stanovení způsobu ověřování při přístupu na zdrojové systémy
- Zajištění seznamu všech zpráv z dokumentace aplikace
- Určení důležitosti zpráv z logů (co se má /nemá sledovat)
- Stanovení minimální požadované míry detailu logování (na úrovni aktiv)
- Ověření, že je ve zdrojích zavedena časová synchronizace, výjimky
- Stanovení způsobu nasazení agenta WinCollect v režimu společného kolektoru či agenta v koncovém systému (minimálně požadavky na instalaci, oprávnění, způsob jeho aktualizace)

2.2. Zjistit nedostatky při logování:

- Některé důležité informace se nelogují
- Není zajištěna dostatečná podrobnost logování
- Logování vyžaduje dodatečný SW, licence apod.
- Logy nejsou dokumentované
- Je vyžadována extra součinnost (práce specialistů) 3. strany.
- Doporučení k odstranění zjištěných nedostatků.

2.3. Stanovit všechny zdroje toků, evidovat je v přehledné tabulce, minimálně bude popsáno:

- Označení, kategorizace a popis zdrojů toků
- Označení IP sítí a jejich hierarchie

2.4. Další různé požadavky.

- Využít identity uživatelů a počítačů.
- Stanovit míru integrace do prostředí ICT Zadavatele k získávání dat do korelací.
- Stanovit požadované pohledy a reporty
- Stanovit požadované reakce na bezpečnostní události
- Stanovit uživatelské role, ověřování a autorizace
- Stanovit způsob a obsah zálohování a obnovy.
- Určit bezpečnostní funkce pro zabezpečení řešení

2.5. Zpracování realizačního projektu:

- Popsat postup implementace v projektu dle projektových fází. Formát dokumentu Microsoft DOC.
- Obsahem musí být minimálně:
  - Projektová organizace, role a osoby na projektu
  - Low level design řešení respektující závěry analýzy dle bodů A1 až A6
  - Požadavky na součinnost
  - Seznam výstupů projektu
  - Etapy a dodávky
  - Harmonogram
  - Akceptace
- Celý dokument Analýza a projekt bude vyhodnocen v oponentuře Zadavatele, až po zapracování připomínek a jejich schválení bude možné začít implementaci.

3. PODROBNÉ TECHNICKÉ POŽADAVKY NA ŘEŠENÍ (TECHNICKÁ SPECIFIKACE):

Řešení musí splňovat všechny následující požadavky.

3.1. Obecné požadavky:

- Řešení musí zajišťovat centrální sběr a zpracování logů, jejich normalizaci, korelaci, grafickou interpretaci a archivaci, centrální správu a reporting, a to včetně vyhodnocení vlastních logů.
- Řešení musí obsahovat inteligenci výrobce SIEM k obraně proti posledním hrozbám ve veřejném internetu (reputační služby), včetně informací o zdrojích malware, spam a botnetech.
- Stávající nastavení z Extreme SIEM V7.2 od Extreme Networks musí být vyhodnocena, aktualizována a zavedena při instalaci nového řešení QRADAR SIEM V7.3 od IBM). Produkt musí být nově instalován a konfigurován do čistého virtuálního prostředí. Stávající výkon řešení je 100 EPS a 15000 FPM.
- Výrobce řešení musí veřejně, srozumitelně a prokazatelně deklarovat vedení produktové a licenční politiky a to včetně všech nabízených funkcionalit. Musí být jasné podmínky, za kterých je možné řešení dále rozšiřovat.
- Řešení musí být postaveno na standardních licencích výrobce, které může dodat libovolný certifikovaný partner výrobce IBM.

3.2. Architektura

- Požadované řešení SIEM je vše v jednom (all-in-one)
- Řešení je postaveno na SW, musí být použita virtualizační vrstva, která zajistí vyšší automatizaci, vizualizaci provozu a komfort obsluhy, proto SIEM musí být ve formě virtuální appliance (vč. software, licencí apod.), požadovaná virtualizační platforma je VMware ESXi/vCenter V5 a vyšší (instalace virtuální appliance prostřednictvím OVA/ISO souboru).
- Pro nasazení virtuální appliance bude Zadavatelem zajištěno odpovídající HW prostředí.

3.3. Škálovatelnost:

- Řešení musí být dobře škálovatelné, aby mohlo růst s počtem nově začleňovaných zdrojů.
- Rozšiřování počtu garantovaných EPS musí být umožněno dokupováním standardních licenčních balíků výrobce IBM alespoň po 100 a 500 EPS.

- Řešení musí být výkonově rozšiřitelné do garantované minimální hodnoty 1000 EPS na základě pouhého dokoupení standardních licenčních balíků výrobce IBM bez jakéhokoliv dodatečného SW.
- Řešení musí být výkonově rozšiřitelné do garantované minimální hodnoty 100 000 FPM na základě pouhého dokoupení standardních licenčních balíků výrobce IBM bez jakéhokoliv dodatečného SW.

3.4. Garance sběru logů z minimálně níže uvedených produktů:

3.4.1. Operační systémy:

Řešení musí obsahovat předefinovaná pravidla výrobcem pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat v připravených v pohledech a reportech, minimálně:

- Microsoft Windows Server 2008, 2012 a 2016
- Microsoft Windows 7 a 10
- Linux všechny běžné edice

3.4.2. Služby a aplikace:

Řešení musí obsahovat předefinované pravidla výrobcem pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně:

- Microsoft AD, print, file, DNS, DHCP a WINS služby
- Microsoft Exchange 2013 a 2016
- Microsoft SharePoint
- Microsoft SQL 2012 a 2014
- Microsoft IIS 6, 7 a 8
- Microsoft ISA
- Microsoft System Center
- Microsoft Hyper-V

- Apache Web server
- Apache TomCat server
- Linux DNS, DHCP

3.4.3. Aplikace „na míru"

Dodavatel musí řešení doplnit o pravidla a nástroje pro načítání a rozparsování logů z interní aplikace „na míru" k zobrazení dat v připravených v pohledech a reportech.
Jedná se o interní chráněnou informaci, kterou Zadavatel poskytne až na základě žádosti uchazeče zaslané na email[redacted]

- Zpracování logů z IS Proxio
- Zpracování logů z eSSL Elisa
- Integrace logů z AV systém ESET

Je požadováno zpracování logů různé struktury z agendového IS úřadu, logy jsou zapisovány do souborů (log soubor) a každá událost (log zpráva) v sobě obsahuje za názvem události i více

specifických víceřádkových výpisů (různé formáty) z komponent tohoto IS (moduly aplikace, java, databáze apod.)
Dodavatel musí připravit externí normalizér (nad rámec standardní funkcionality SIEM) nutný předzpracování logů pro vyhodnocení v SIEM. Normalizér načítá logy ukládaných do log souboru v IS Proxio, ořezává log zprávy na základní monitorovanou událost, zbytek specifického obsahu log zpráv maže, oříznuté log zprávy opět ukládá do log souboru, odkud pak SIEM načítá normalizované log soubory se zkrácenými log zprávami pro vlastní standardní zpracování.

3.4.4. Infrastruktura:

Řešení musí obsahovat předefinované pravidla výrobcem pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně:

- Aktivní prvky HPE (switche, routery, wireless zařízení)
- Aktivní prvky Mikrotik (switche, routery, wireless zařízení)
- Aktivní prvky Cisco (switche, routery, wireless zařízení)

- VMware ESXi V5 a vyšší
- VMware vSphere V5 a vyšší
- VMware vCenter V5 a vyšší
- VMware vShield

- HPE a Synology diskové úložiště
- HPE server management

- APC UPS
- Eaton UPS management
- Sentinel UPS management

3.4.5. Databáze

Řešení musí obsahovat předefinované pravidla výrobcem pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně:

- Microsoft SQL 2012 a 2014
- Oracle
- MySQL
- Informix 11
- PostgreSQL

3.4.6. Bezpečnostní technologie

Řešení musí obsahovat předefinované pravidla výrobcem pro rozpoznání následujících zdrojů logů a rozparsování logů k zobrazení dat připravených v pohledech a reportech, minimálně:

- Check Point NG Firewall
- Microsoft firewall
- Linux IP tables

- Microsoft Security Event Log
- Microsoft IAS
- Microsoft CA
- Antivir ESET

3.5. Způsoby sběru dat:

Řešení musí podporovat příjem/stahování logů z požadovaných zdrojů logů, minimálně podpora následujících protokolů:

- Syslog
- Forwarded syslog
- TCP/UDP multiline syslog
- TLS syslog
- JDBC
- ODBC
- OPSEC LEA
- HTTP Receiver
- Cisco NSEL
- EMC VMware
- Oracle DB Listener
- SDEE
- SMB Tail
- Log File
- SNMP v1, v2, v3
- Microsoft Event Log over MSRPC

Řešení musí podporovat Flow protokoly:

- Netflow v1, v3, v7 a v9
- Jflow
- Sflow v2, v4 a v5
- IPFIX
- Flowlog file
- Qflow

Řešení musí podporovat import dat ze skenerů zranitelností následujících předních výrobců:

- Nessus Scanner
- Qualys
- Rapid7 Nexpose Scanner

Je požadována podpora vyčítání vzdálených souborů s logy (Log Files), minimálně prostřednictvím bezpečných protokolů:

- SCP
- SFTP

Příjem toků ze zrcadlených zdrojů toků, minimálně podpora:

- Zrcadleného provozu (toků) z prvků LAN sítě (funkce Port Monitoring)
- Monitoring min. 2x 10 GE fyzických rozhraní z centrálního prvku Zadavatele

3.6. Specifikace sběru logů a toků

- Je požadováno automatické rozpoznání zdrojů logů (vč. typu zařízení a výrobce) u globálně rozšířených produktů.
- Je požadováno začlenění i specifických zdrojů logů (např. aplikací vytvořených „na míru") prostřednictvím univerzálního profilu, který umožní pojmenování a dodatečnou konfiguraci těchto zdrojů logů.
- Naučení specifických zdrojů logů musí být prováděno jen prostřednictvím jednotného GUI SIEM.
- Je požadováno vyhodnocení datových toků na aplikační úrovni, uživateli musí být umožněn náhled do aplikačního obsahu datové komunikace (ISO OSI L7 analýza).
- Díky ISO OSI L7 analýze musí být z obsahu jasné, jaké řídící příkazy aplikační protokol používá, minimálně: FTP, POP3, Telnet, SMTP, HTTP, SIP.
- Zobrazení aplikačního obsahu z analýzy toků musí být dostupné prostřednictvím jednotného GUI SIEM.
- Je požadováno vyhodnocení logů a toků společně se zjištěnými technickými zranitelnostmi.
- Je požadována podpora importovaných scoringu zranitelností na základě obecného standardu Common Vulnerability Scoring System (CVSS).
- Je požadováno doplňování informací o uživatelích a počítačích ze systému identit (minimálně jméno účtu uživatele, jméno uživatele a jméno počítače).
- Řešení musí poskytovat sběr logů ze všech požadovaných zdrojů i bez jakýchkoliv instalovaných agentů ve zdrojích logů (bez agentský sběr)
- Je požadována podpora zpracování více řádkového logu (multi-line Syslog).
- Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při komunikaci se zdroji dat, tak i při normalizaci vstupních dat
- Systém SIEM nesmí být licenčně omezen na počet zařízení generujících logy (zdrojů logů), na počtu evidovaných aktiv a na počtu uživatelů/konzolí
- Systém SIEM nesmí technicky limitovat počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, aby nedošlo k jejich zahození

3.7. Zpracování logů a toků:

- Řešení musí obsahovat přednastavená korelační pravidla, která řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z následujících oblastí:
  - Útoky červů, virů a robotů
  - Neoprávněný přístup vč. ověřování, změny konfigurace
  - Chyby a změny v sítích vč. chyb a stavů síťových zařízení
  - Monitorování aktiv vč. aktivit privilegovaných uživatelů, přístupů a změn konfigurací, odmítnutých připojení, úspěšných a chybných přihlášení a hlášení systémů IPS/IDS)
  - Překročení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla a změny konfigurace)
- Řešení musí korelovat minimálně položky: zdrojová IP, cílová IP, zdrojový port, cílový port, uživatelské jméno, jméno účtu, jméno počítače, jméno události, kategorie události, čas přijetí, čas vygenerování, MAC, surová data.
- Řešení musí podporovat doplnění údajů do korelovaných výstupů z připravených číselníků.
- Řešení musí umožňovat definici vlastního (custom) atributu (číselného a textového) v událostech, do kterého je automaticky doplňována hodnota z externího zdroje.
- Výsledkem korelace je standardní událost v rámci SIEM, která může být dále použita i jako základ pro další korelace a vznik kumulovaných událostí.
- Součástí korelace musí být i informace z integrovaných globálních reputačních služeb výrobce.
- Řešení musí korelovat dohromady události z logů a toků (vč. zrcadleného toku a NetFlow/IPFIX)
- Řešení musí umožnit definovat vlastní (custom) pravidla pro vyhodnocování anomálií i v síťovém provozu.

- Vlastní (custom) atribut musí být použitelný pro filtraci, drill-down i definice korelací napříč celým SIEM.
- Výsledky scanneru zranitelností se automaticky korelují do korelovaných událostí.
- V případě zaznamenání útoku, musí dojít ke korelaci informací ze scanneru ohledně zjištěných zranitelností v interních aktivech, SIEM pak musí určit, zdali byl útok na dané aktivum úspěšný či nikoliv.
- Je požadována možnost integrované analýzy chování uživatelů a strojových identit (tzv. UEBA/UBA), tyto události a anomálie musí být vyjádřené graficky prostřednictvím prioritizovaných přehledů a grafů
- Řešení musí provádět evidenci aktiv v SIEM s informací o jejich geografickém umístění a zobrazení na mapě, to platí i o vizualizaci vzniklých (korelovaných) událostí na geolokační mapě
- Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup)
- Je požadováno intuitivní prostředí (průvodce) k přidávání a změně log parserů prostřednictvím jednotného GUI SIEM bez nutnosti spolupráce s dodavatelem nebo výrobcem
- Konfigurace integrovaného parsovacího nástroje k naučení specifických zdrojů logů musí být prováděna pouze prostřednictvím jednotného GUI SIEM.
- Je požadováno intuitivní prostředí (průvodce) k přidávání a změně vlastních korelačních pravidel prostřednictvím jednotného GUI SIEM bez nutnosti spolupráce s dodavatelem nebo výrobcem

3.8. Pohledy na data (informace):

- Řešení musí poskytovat grafický dashboard (grafickou pracovní plochu) libovolně konfigurovatelný pro každého uživatele SIEM zvlášť dle náplně práce a geografického uspořádání ICT.
- Dashboardy musí umožňovat jejich stavbu z minimálně následujících typů grafů:
  - Graf v závislosti na čase
  - Koláčový graf
  - Tabulkový výpis
  - Sloupcový graf
- Grafy v dashboardech musí umožňovat výběr určité své části pro rychlé vymezení oblasti vyhledávaných událostí.
- Je požadována analýza dat v reálném čase a jejich zobrazení pomocí GUI prohlížeče.
- Jsou vyžadovány minimálně následující pohledy:
  - Bezpečnost = stav bezpečnosti a detekované incidenty
  - Autentizace = kdo, kdy, kde se přihlásil
  - Uživatelská aktivita = co dělal vybraný uživatel
  - Využívání sítě
  - Využívání aplikací
  - Shoda s pravidly = který počítač porušuje pravidla = využívá závadný obsah, provozuje nepovolené programy, služby a aplikace, komunikuje nepovolenými protokoly, komunikuje se zakázanými cíly apod.
  - Audit = kdo, kdy a jak změnil nastavení systému
- Řešení musí umožnit pohled na korelované události v reálném čase včetně nastavení vlastních vyhledávání a filtrů.
- Řešení musí umožnit pohled na korelované historické události včetně nastavení vlastních vyhledávání a filtrů.
- Řešení musí obsahovat v dashboardu pohled na časově nejbližší korelované událostí.
- Řešení musí obsahovat v dashboardu pohled na nejvýznamnější korelované události.

- Řešení musí umožnit pohledy na sběr logů a toků podle typu aktiv, typu událostí, libovolného časového období a míry detailu/abstrakce.
- Každý uživatel musí být schopen si vytvářet vlastní dashboardy podle jemu svěřené agendy
- Řešení musí podporovat vyhledávání logů/eventů na základě „full-text" indexace
- Řešení musí podporovat vyhledávání a filtrování prostřednictvím jednotného GUI SIEM

3.9. Reakce:

- Podpora varování (alerting) na zjištěné bezpečnostní události:
  - Přímo v GUI SIEM
  - E-mailem uživateli
  - SNMP trap / inform do dalších zařízení (bezpečnostní prvky a management nástroje)
  - Skriptem ke spuštění operací v externích zařízeních a aplikacích
- Řešení musí v sobě obsahovat interní skriptovací jazyk k vytvoření reakce na na-míru při události, minimálně podpora Bash, Python a Perl.
- Řešení musí obsahovat funkcionalitu ticketovacího systému, která umožní přiřazovat události k řešení jednotlivým uživatelům (řešitelům), v jednotném GUI SIEM je viditelný stav jejich řešení.

3.10. Ověřování:

- Je požadováno ověřování uživatelů proti interní databázi.
- Je požadováno proti externímu ověřovacímu serveru na základě metod LDAP/Microsoft AD, RADIUS a pomocí prostředků více faktorového ověřování.

3.11. Reporting:

- Řešení musí obsahovat předdefinované a upravitelné reporty
- Řešení musí umožnit definici vlastních reportů typu denní, týdenní, měsíční
- Součástí řešení musí být průvodce k vytváření vlastních (custom) reportů „na míru", který je součástí jednotného GUI SIEM.
- Reporty musí být k dispozici v jednotném GUI SIEM a musí být možné je zasílat uživateli e-mailem.
- Řešení musí být schopno generovat reporty obsahující kterékoliv hodnoty z korelovaných položek.
- V řešení jsou vyžadovány minimálně následující denní reporty:
  - Autentizace = kdo, kdy, kde a jak se přihlásil
  - Uživatelská aktivita = co dělal vybraný uživatel
  - Shoda s pravidly = který počítač porušuje pravidla = např. využívá mravně závadný obsah či nepovolené aplikace
  - Audit = kdo a kdy změnil nastavení systému
  - Bezpečnost = detekované incidenty dle závažnosti, důvěryhodnosti, relevance
  - Využití sítě
  - Využití aplikací
- Systém vytváří reporty ve formátech PDF, HTML a CSV, popř. dalších
- Systém musí umožňovat export dat ve formátu XML nebo CSV

3.12. Jednotné webové GUI SIEM:

- Produkt musí mít kompletní centrální grafické uživatelské rozhraní (GUI) vzdáleně přístupné prostřednictvím běžného webového klientského prohlížeče (Firefox, Chrome, Internet Explorer).
- GUI musí být jednotné, nesmí vyžadovat doplnění dodatečných technologií, instalaci pluginů nebo instalaci „tlustého" klienta.
- Je požadována podpora přístupu uživatelů do GUI systému dle rolí (RBAC), minimálně administrátor (může vše), operátor (může ladit), prohlížeč (nemůže nic měnit).

- Jakmile se uživatel přihlásí do GUI, musí být ověřen a autorizován pro práci s ním. GUI a jeho všechna webová okna využívají úvodní přihlášení bez nutnosti jakékoliv dodatečné autentizace při práce s více okny v SIEM (SSO).
- Podpora autorizace a řízení přidělování oprávnění na úrovni jednotlivých pohledů, reportů, zdrojů a IP sítí.
- GUI musí být jednotné jak pro vyhodnocení logů a toků, přehled korelovaných událostí, tak konfiguraci samotného SIEM.
- V GUI musí být grafický okamžitý a dlouhodobý přehled o výkonu systému z pohledu hodnot EPS a FPM.
- Řešení musí podporovat úpravu přihlašovací stránky GUI vč. vlastního přihlašovacího informačního banneru a vlastního loga.

3.13. Dostupnost systému, zálohování a archivace:

- Řešení musí poskytovat plánované automatizované i manuální zálohy dat a konfigurace, nastavení funkcí zálohování musí být prováděno jen prostřednictvím jednotného GUI SIEM.
- Je požadována podpora flexibilní retenční politiky k nastavení archivace logů na základě různých typů zdrojů logů a jejich důležitosti.
- Je požadována podpora funkce k zajištění integrity uložených logů a toků (hashování), možnost aktivace algoritmu SHA-512 nebo vyššího/bezpečnějšího prostřednictví jednotného GUI SIEM.
- Nativní podpora funkce k zajištění důvěrnosti uložených logů a toků v SIEM (šifrování), možnost aktivace algoritmu HMAC SHA-512 nebo vyššího/bezpečnějšího prostřednictví jednotného GUI.
- Řešení musí umožňovat archivovat originální (neagregované) logy po volně definovanou dobu.
- Je požadována podpora uložení archivu na externím diskové úložiště a zpětné načtení archivu do SIEM.

3.14. Aktualizace SIEM:

- Výrobce řešení musí poskytovat automatické aktualizace systému, které musí minimálně obsahovat:
  - Nové metody detekce porušení bezpečnosti (threat-inteligence)
  - Podporu nově uvolňovaných zařízení 3tích stran jakožto zdrojů logů
  - Nové verze, nová funkcionalita
  - Opravy chyb
- Produkt musí podporovat nastavení periody dotazování aktualizací, které typy aktualizací mohou být prováděny bezobslužně

3.15. Bezpečnost SIEM

- Řešení SIEM musí být bezpečné, výrobce SIEM musí aplikovat globální bezpečnostní standardy a best-practices, bezpečnost SIEM musí vycházet z ISO/IEC 15408, kdy samotný produkt SIEM musí mít **platný certifikát Common Criteria** vydaný patřičným certifikačním úřadem, vydaný certifikát nesmí být starší více než 2 roky. Certifikát musí uchazeč přiložit k podané nabídce.
- Výrobce SIEM musí provozovat vlastní CERT/CSIRT, kdy v případě zjištění bezpečnostních zranitelností v produktu SIEM automaticky elektronicky notifikuje uživatele, oznámí jejich označení a závažnost prostřednictvím CVE a CVSS, poskytne postupy k dočasnému a finálnímu odstranění těchto zranitelností.

4. ROZŠÍŘENÁ SERVISNÍ PODPORA ŘEŠENÍ

Zhotovitel je povinen poskytovat rozšířenou podporu v délce 4 let minimálně v tomto rozsahu:

- dostupnost Helpdesk 8x5 (pracovní dny 9.00 – 17.00)

- doba reakce NBD
- vyhodnocování problémů (SW vada, výkonnostní problém atp.) přes vzdálený přístup
- aktivní řešení chyb a vad s podporou výrobce
- migrace systému v případě selhání (obnovení ze zálohy, import dat)
- přístup k posledním verzím SW, pravidelné instalace updatů a oprav tak, jak jsou postupně uvolňovány výrobcem
- údržba řešení k zajištění bezchybného a efektivního chodu
- odstranění závad či chyb nahlášených či požadovaných objednatelem
- zvýšená poimplementační podpora po dobu 1 měsíce od implementace pro přednostní řešení nestandardních stavů způsobených implementací.

Dále zhotovitel poskytne konzultace a rozvoj nad rámec servisní podpory v rozsahu 12 MDs za rok pro:

- pomoc se zavedením nových zdrojů logů do řešení
- analýzu logovaného provozu, definovaní či zpřesnění nastavení
- úpravu pravidel, reportů, dashboards apod.
- kontrolu integrovaných aplikací vytvořených „na-míru"
- pomoc s řešením zjištěných bezpečnostních událostí/incidentů

Rozšířená podpora bude specifikována v samostatné smlouvě o provádění technického servisu.

5. ŠKOLENÍ

- Součástí dodávky Uchazeče musí být školení uživatelů (správců) Zadavatele cílené na obsluhu a správu dodávaného řešení v délce 8 hodin.
- Školení bude provedeno Uchazečem v místě sídla Zhotovitele.

6. POUŽITÉ ZKRATKY

AD – Active Directory
AV - Antivirus
CA – Certification Authority
CERT - Computer emergency response team
CLI – Command Line Interface
CPU – Central Processor Unit
CSIRT - Computer security incident response team
CSV – Comma Separated Value
CVE – Common Vulnerabilities and Exposures
CVSS – Common Vulnerability Scoring System
DB – Database
DNS – Domain Name System
DHCP – Dynamic Host Configuration Protocol
EPS – Event per Second
FPM – Flow per Minute
FTP – File Transfer Protocol
GB – Giga Byte
GE – Gigabit Ethernet
GHz – Giga Hertz
GUI – Graphical User Interface
HA – High Availability
HTTP – Hyper Text Transfer Protocol
HMAC – Hash-based Message Authentication Code

HW – Hardware
IAS – Internet Authentication Service
ICT – Information and Communication Technology
IEC – International Electrotechnical Commission
IDS – Intrusion Detection System
IP – Internet protocol
IPS – Intrusion Protection System
IIS – Internet Information Server
IS – Information System
ISO - International Organization for Standardization
JDBC - Java Database Connectivity
Lx – Layer (x)
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
MAC – Media Access Control
MSPC – Microsoft Remote Procedure Call
NAC – Network Access Control
NG – Next Generation
NSEL – NetFlow Secure Event Logging
ODBC – Open Database Connectivity
OPSEC – Open Platform for Security
OSI – Open System Interconnection
OVA – Open Virtualization Appliance
PDF – Portable Document Format
POP3 – Post Office Protocol 3
RADIUS – Remote Authentication Dial In User Service
RAM – Random Access Memory
RBAC – Role Base Access Control
SCOM – System Center Operations Manager
SCP – Secure Copy Protocol
SDEE – Security Device Event Exchange
SFTP – Secure File Transfer Protocol
SHA – Secure Hash Algorithm
SIEM – Security Information and Event Monitoring
SIP – Session Initiation Protocol
SMB – Server Message Block/Samba
SNMP – Simple Network Management Protocol
SQL – Structured Query Language
SSO – Single Sign On
SW – Software
TB – Terra Byte
TCP – Transmission Control Protocol
TLS – Transaction Layer Security
UBA – User Behavior Analytics
UDP – User Datagram Protocol
UEBA – User and Entity Behavior Analytics
UPS – Uninterruptible Power Supply
WINS – Windows Internet Name Service
WLAN – Wireless LAN
WMI – Windows Media Instrumentation
XML – Extensible Markup Language

Příloha č. 2 – Časový harmonogram realizace díla

Město Sokolov - Implementace upgrade systému monitorování bezpečnostních incidentů a události												
č.	*popis činnosti*	*konec činnosti*	T0	T1	T2	T3	T4	T5	T6	T7	T8	T9
1	uzavření smluvního vztahu	T0										
2	zpracování předimplementační analýzy a realizačního projektu	T0+3týdny										
3	odsouhlasení analýzy a zajištění připravenost pro SIEM	T0+4týdny										
4	dodávka SIEM řešení, vč. předplacené podpory výrobce na 4 roky	T0+6týdnů										
5	dodání implementační dokumentace	T0+6týdnů										
6	proškolení uživatelů (správce)	T0+7týdnů										
7	akceptační testy, akceptace projektu, fakturace	T0+7týdnů										
8	zahájení 4-leté servisní podpory SIEM	T0+8týdnů										
9	zkušební provoz - volitelná položka	T0+9týdnů										
10	odstraňování případných výhrad	T0+9týdnů										
11	úplné ukončení implementačního projektu	T0+10týdnů										

Příloha č. 3 – Specifikace součinnosti ze strany Objednatele

Součinnost: Specifikace součinnosti za strany Zadavatele:

- Podání žádosti o uzavření smlouvy IBM Passport Advantage program pro Government s výrobcem SIEM (společností IBM) a uzavření této smlouvy

Poznámka: Uzavření této smlouvy je podmínkou pro dodržení nabídnutých cen – jedná se o speciální ceny určené pro státní správu, jejichž poskytnutí ze strany výrobce je podmíněno uzavřením této smlouvy.

- Vytvoření/aktualizace seznamu aktiv (zdrojů logů) s jejich specifikací k logování do SIEM:
  - Typ/označení aktiva
  - Výrobce aktiva
  - IP adresa
  - Jméno
  - Protokol ke sběru logů
  - Účet (jen metoda „pull")

Poznámka: bude použit stávající seznam zdrojů logů ze stávajícího SIEM rozšířený o nová aktiva, seznam bude zaveden do nového SIEM.

- Vytvoření/aktualizace síťové hierarchie:
  - IP sítě
  - Jména sítí
  - Shluky aktiv podle účelu (např. DNS, mail servery apod.)

Poznámka: bude použit stávající seznam ze stávajícího SIEM rozšířený o nová aktiva, seznam bude zaveden do nového SIEM.

- Přidělení IP adresy pro nový SIEM (dočasná, nebude určena ke sběru logů)
- Vzdálený přístup VPN pro konfiguraci řešení a vzdálenou správu
- Zajištění virtuálního prostředí VMware pro SIEM:
  - Samostatná instance (VM) pro nový SIEM
  - Platforma ESXi/vCenter V5 a vyšší
- Zajištění odpovídajícího výpočetního výkonu a úložné kapacity:
  - 32GB vRAM nebo více
  - 8 vCPU nebo více
  - Úložná kapacita dle dohody
- Oponentura připraveného postupu a technických parametrů před zahájením instalace
- Spuštění ISO souboru ve VMware
- Zajištění konfigurace nových zdrojů logů (na straně zdrojů logů)
- Zajištění přístupu do internetu pro aktualizace SIEM
- Zajištění konektivity ke všem zdrojům logů (aktivům)

Poznámka: Po dobu migrace budou v běhu obě instance. Nastavení SIEM bude postupně migrována. V okamžiku migrace budou zaměněny IP adresy obou SIEM instancí, aby byl minimalizován dopad migrace (změny) na zdrojové systémy. Stará instance SIEM bude odstavena od sběru logů a zanikne až po stanovené době retence logů určené Zadavatelem.

Spolupráce při přejímkách, testování a akceptaci

Příloha č. 4 – Seznam zástupců

Seznam zástupců ze strany Zhotovitele

	Vedoucí projektového týmu	Technický specialista	Konzultant bezpečnosti
Jméno a příjmení	[redacted]		
Pracovní pozice a druh práce	Projektový manažer, Řízení projektů formou projektového řízení, koordinace projektu	Technik specialista, analýza, design, implementace a podpora SIEM	Konzultant informační bezpečnosti

Seznam zástupců ze strany Objednatele

	Vedoucí projektového týmu	Technický specialista	Konzultant bezpečnosti
Jméno a příjmení	[redacted]		

Příloha č. 5 – Položkový rozpočet - vlastní cenová nabídka zhotovitele

Upgrade licencí SIEM - Licence a 1. rok podpory a služeb výrobce

1	D1RNCLL	IBM QRadar Software Install License + SW Subscription & Support 12 Months (Entitlement includes base capacity of 100 events per second (EPS) and 15,000 flows per minute (FPM) for use within the deployment.)	9 203,00 €	30,00%	6 442,10 €	169 556,07 Kč
1	D1S2ILL	IBM QRadar Software Node Install License + SW Subscription & Support 12 Months	845,00 €	30,00%	591,50 €	15 568,28 Kč

Pozor: pro získání slevy pro SŠ/VŠ je nutné podepsat s IBM Passport Advantage program pro Government

Upgrade licencí SIEM - 2-4. rok podpory a služeb výrobce

1	E0NBALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months (2nd year)	1 840,00 €	28,00%	1 324,80 €	34 868,74 Kč
1	E0NEGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months (2nd year)	169,00 €	28,00%	121,68 €	3 202,62 Kč
1	E0NBALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months (3rd year)	1 840,00 €	25,74%	1 366,38 €	35 963,23 Kč
1	E0NEGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months (3rd year)	169,00 €	25,74%	125,50 €	3 303,14 Kč
1	E0NBALL	IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months (4th year)	1 840,00 €	18,30%	1 503,28 €	39 566,33 Kč
1	E0NEGLL	IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months (4th year)	169,00 €	18,30%	138,07 €	3 634,08 Kč

Pozor: pro získání slevy pro SŠ/VŠ je nutné podepsat s IBM Passport Advantage program pro Government

Upgrade licencí SIEM - realizace změny dodavatelem

1	Příprava realizace změny (dokumemtace, postup, harmonogram, součinnost, akceptační testy) Provedení instalace a konfigurace SW - reinstalace, přenesení veškeré konfigurace vč. všech stáv. zdrojů logů Provedení akceptačních testů Zaškolení správců (změna) Aktualizace stáv. provozní dokumentace	66 060,00 Kč	10,0%	59 454,00 Kč	59 454,00 Kč
1	Řízení projektu (projektový manažer)	6 606,00 Kč	10,0%	5 945,40 Kč	5 945,40 Kč

Upgrade licencí SIEM - rozšířená měsíční podpora dodavatele (cena za měsíc)

48	Rozšířená měsíční podpora dodavatele vč.: Povyšování verzí (patche), záloha konfigurace HelpDesk, CallDesk, režim 5x8, reakce do 4 hod Komunikace s výrobcem za zákazníka při řešení problémů Roční preventivní kontrola stavu řešení na místě	4 128,75 Kč		198 180,00 Kč	198 180,00 Kč

Jednorázová cena	
Jednorázová cena v CZK bez DPH	569 242,00 Kč
Jednorázová cena DPH v CZK	119 541,00 Kč
Jednorázová cena v CZK včetně DPH	688 783,00 Kč