SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená dle ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

I.
Smluvní strany

Níže uvedeného dne, měsíce a roku spolu smluvní strany

Městská část Praha 11

se sídlem:	Ocelíkova 672/1, 149 41 Praha 4
IČO:	00231126
DIČ:	CZ00231126
zastoupena:	Jiřím Dohnalem, radním MČ Praha 11
bankovní spojení:	[redacted]
číslo účtu:	

(dále jen „Objednatel")

a

Next Generation Security Solutions s.r.o.

se sídlem:	U Uranie 954/18, Holešovice, 170 00 Praha 7
IČO:	06291031
DIČ:	CZ06291031
zastoupena:	Mgr. Ondřejem Dedkem, jednatelem
bankovní spojení:	[redacted]
číslo účtu:	

Společnost zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, oddíl C, vložka 279627

(dále jen „Poskytovatel"); (společně též „smluvní strany")

uzavřely tuto Smlouvu (dále jen „Smlouva").

II.
Předmět Smlouvy

1. Předmětem této Smlouvy je poskytování služeb spočívajících v zajištění provozu a bezpečnosti Log managementu infrastruktury z kritických systémů a aplikací Objednatele, a to v souladu s podmínkami této Smlouvy a se zadávacími podmínkami veřejné zakázky na tyto služby s názvem **„Logmanager"**, v jejímž rámci je tato Smlouva uzavírána (dále jen „Služba"). Podrobná specifikace poskytovaných Služeb je vymezena v příloze č. 1 této Smlouvy – Technická specifikace.
2. Součástí poskytovaných Služeb je dodávka a implementace systému nutného ke splnění předmětu plnění plynoucího z odst. 1 této Smlouvy (dále „Systém") a rovněž podpora provozu Systému a poskytování operativních služeb po dobu 12 měsíců.
3. Smluvní strany berou na vědomí, že pokud není dále v této Smlouvě nebo v příloze stanoveno jinak, budou Služby primárně poskytovány vzdáleně. Za tímto účelem se Objednatel zavazuje umožnit Poskytovateli vzdálený přístup do sítě, aplikací, systémů apod. a to v rozsahu, který je nutný nebo vhodný pro řádné plnění povinností Poskytovatele dle této Smlouvy. V případě, že nebude možné nebo vhodné poskytovat některé ze Služeb prostřednictvím vzdáleného přístupu, je Objednatel povinen poskytnout Poskytovali nezbytnou součinnost a umožnit mu přístup do prostor, serverů a počítačů atd. za účelem plnění této Smlouvy.
4. Smluvní strany berou na vědomí, že zcela zásadní pro řádné plnění Smlouvy je součinnost Objednatele. Objednatel je povinen předávat Poskytovateli kromě přístupů do systémů, především informace a podklady v rozsahu odpovídajícím Službám dle této Smlouvy. V případě jakékoliv změny nebo nové informace je Objednatel povinen tuto změnu nebo informaci bezodkladně sdělit Poskytovateli a případně mu k tomu poskytnout doklady a/nebo další informace.

III.
Termín poskytnutí služeb a místo plnění

1. Předání Systému: do 31. 12. 2023
2. Poskytování Služeb: 1. 1. 2024 – 31. 12. 2024
3. Místo plnění: sídlo Objednatele

IV.
Cena a platební podmínky

1. Cena za Systém a poskytování Služeb (dále jen „Cena") blíže upřesněných v příloze č. 1 byla dohodou smluvních stran stanovena takto:

Celková Cena bez DPH	**1 179 300 Kč**
DPH	247 653 Kč
Celková Cena včetně DPH	1 426 953 Kč

2. Cena uvedená v odst. 1 tohoto článku je konečná a maximální a může být měněna pouze v souvislosti se změnou sazeb DPH či jiných daňových předpisů majících vliv na cenu předmětu Smlouvy. Rozhodným dnem pro změnu Ceny z důvodu zákonné změny sazby DPH je den účinnosti takové změny.
3. Objednatel se zavazuje uhradit Cenu po protokolárním předání a převzetí Systému na základě daňového dokladu (faktury) vystavené Poskytovatelem.
4. K Ceně bude připočtena daň z přidané hodnoty v souladu s platnými právními předpisy.
5. Objednatel se zavazuje uhradit Cenu přímou platbou na bankovní účet Poskytovatele na základě Poskytovatelem vystaveného daňového dokladu (faktury) v souladu s příslušnými ustanoveními zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. Při zasílání faktur musí být respektována sjednaná adresa dle odst. 9 tohoto článku smlouvy, na každé faktuře musí být mj. uvedena informace o čísle této smlouvy SM2300001160 a dále, že objednatelem budou provedené práce hrazeny z bankovního účtu č. [redacted]
6. Uhrazením faktury se rozumí její připsání na účet Poskytovatele uvedený na daňovém dokladu (faktuře). Splatnost faktur činí 21 dnů ode dne doručení daňového dokladu Objednateli.
7. V případě prodlení s úhradou daňového dokladu (faktury) nebo její části má Poskytovatel nárok na úrok z prodlení v zákonné výši.
8. Cena bude hrazena bez poskytování záloh.
9. Adresa pro zasílání faktur: Městská část Praha 11, Ocelíkova 672/1, 149 41 Praha 4,
   e-mail: [redacted]

V.
Další povinnosti smluvních stran

1. Poskytovatel je povinen dodržovat právní a technické podmínky vyplývající ze závazných platných právních předpisů, vyhlášek a norem.
2. Poskytovatel je povinen zajistit autorskoprávní nezávadnost plnění. Pokud Poskytovatel při plnění této Smlouvy užije výsledek činnosti třetího subjektu chráněný právem průmyslového nebo jiného duševního vlastnictví, autorským právem apod., a uplatní-li oprávněná osoba z tohoto titulu své nároky vůči Objednateli, Poskytovatel provede na své náklady vypořádání majetkových důsledků a je odpovědný za jakoukoli újmu způsobenou Objednateli.

VI.
Předání a převzetí Systému

1. Předání a převzetí Systému bude sepsáno a potvrzeno předávacím protokolem vyhotoveným za součinnosti obou smluvních stran.
2. U předávacího řízení je Poskytovatel povinen doložit veškeré potřebné doklady. V případě dodávky Systému jde zejména o:
   - doklad o souladu Systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

VII.
Odpovědnost za vady

1. Poskytovatel odpovídá za odbornou úroveň poskytovaných Služeb dle této Smlouvy. Právo na náhradu újmy vzniklé neodborným provedením poskytovaných Služeb se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2. Poskytovatel tímto čestně prohlašuje, že má oprávnění k činnosti v rozsahu této Smlouvy a je účasten pojištění z odpovědnosti za újmu vzniklou jinému v souvislosti s poskytováním služeb.
3. Poskytovatel poskytuje na provedení Služeb záruku v délce 12 měsíců, která začíná běžet ode dne předání každé jednotlivé Služby. Poskytovatel je povinen odstranit vady každé jednotlivé Služby, tj. odchylky od výsledku stanoveného touto Smlouvou, které se projeví v průběhu trvání záruční doby. Objednatel je povinen uplatňovat u Poskytovatele práva z poskytnuté záruky písemně, nejpozději do 30 dnů po zjištění vad, na něž se záruka vztahuje. Poskytovatel je povinen vadu odstranit bezodkladně, nejpozději do jednoho měsíce od obdržení písemnosti, ve které je záruka uplatňována, nedohodnou-li se strany jinak.

VIII.
Další ujednání

1. Smluvní strany se zavazují, že bez předchozího písemného souhlasu druhé strany nevyzradí třetím osobám technické ani obchodní informace druhé strany, které se dozvěděly v souvislosti s plněním dle této Smlouvy.
2. Poskytovatel se zavazuje (v prostorách a na pracovištích Objednatele) postupovat při plnění této Smlouvy s odbornou péčí a zavazuje se dodržovat právní a technické předpisy a ostatní podmínky uložené mu Smlouvou nebo veřejnoprávními orgány tak, aby byla zajištěna bezpečnost pracovníků Poskytovatele a třetích subjektů po celou dobu poskytování služeb.
3. Poskytovatel je povinen upozornit Objednatele ihned na nesprávnost jeho pokynů nebo podkladů, jinak odpovídá Objednateli za újmu tím způsobenou.
4. Poskytovatel i Objednatel jsou povinni se navzájem informovat o tom, že se dostali do úpadku ve smyslu § 3 zák. č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů.

IX.
Odstoupení od Smlouvy

1. Pro účely odstoupení od Smlouvy se za podstatné porušení Smlouvy považuje zejména:
   - vadnost poskytovaných Služeb již v průběhu jejich provádění, pokud Poskytovatel na písemnou výzvu Objednatele vady neodstraní ve lhůtě výzvou stanovené,
   - úpadek Objednatele ve smyslu § 3 zák. č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů,
   - zahájení insolvenčního řízení, ve kterém je Poskytovatel v postavení dlužníka.
2. Dojde-li k výše uvedenému porušení Smlouvy, je příslušná smluvní strana oprávněna od Smlouvy odstoupit. Odstoupení od Smlouvy musí být učiněno písemnou formou. V takovém případě nastávají účinky odstoupení od Smlouvy dnem, ve kterém smluvní straně dojde oznámení o odstoupení ve smyslu § 570 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Od Smlouvy je možné odstoupit jak bez zbytečného odkladu, tak i v případě, pokud důvod, pro který je odstupováno, stále přetrvává.
3. Odstoupením od této Smlouvy z důvodů uvedených v odst. 1 této Smlouvy nezaniká povinnost k náhradě způsobené újmy.

X.
Důvěrnost informací

1. Smluvní strany jsou si vědomy toho, že v rámci plnění Smlouvy:
   - si mohou vzájemně poskytnout informace, které budou považovány za důvěrné (dále důvěrné informace),
   - mohou jejich zaměstnanci získat přístup k důvěrným informacím druhé strany.
2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany. S výjimkou plnění této Smlouvy, se obě strany zavazují nepublikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli splnit Smlouvu. Obě strany se zároveň zavazují nepoužít

důvěrné informace druhé strany jinak než za účelem plnění Smlouvy nebo uplatnění svých práv z této Smlouvy.

3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, 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 a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit újmu.
4. Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.
5. Ustanovení tohoto článku není dotčeno ukončením účinnosti Smlouvy z jakéhokoliv důvodu a jeho účinnost skončí nejdříve deset (10) let po ukončení účinnosti této Smlouvy.

XI.
Závěrečná ustanovení

1. Vztahy plynoucí z této Smlouvy a vztahy neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2. Smluvní strany se dohodly, že tato Smlouva je veřejně přístupnou informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
3. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv postupem dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, a její zveřejnění zajistí Objednatel.
4. Žádná ze smluvních stran není oprávněna postoupit práva či pohledávky nebo převést závazky z této Smlouvy vyplývající na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany. Práva i povinnosti ze Smlouvy přecházejí na právní nástupce obou stran. Obě strany jsou povinny informovat se navzájem o takových změnách.
5. Tuto Smlouvu lze měnit pouze písemnou formou číslovanými dodatky podepsanými oběma smluvními stranami.
6. Tato Smlouva je podepsaná vlastnoručně a je vyhotovena ve pěti (5) stejnopisech, z nichž Objednatel obdrží tři vyhotovení a Poskytovatel dvě vyhotovení.
7. Doložka dle zákona o hl. m. Praze: uzavření této Smlouvy schválila RMČ usnesením č. 1278/56/R/2023 ze dne 13.12.2023 a k jeho podpisu je pověřen Jiří Dohnal, radní MČ Praha 11, na základě usnesení RMČ č. 1278/56/R/2023 ze dne 13.12.2023.
8. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, bezvýhradně souhlasí s jejím obsahem a že ji uzavírají ze své vážné a svobodné vůle, prosté omylu. Na důkaz toho připojují podpisy svých oprávněných zástupců.
9. Nedílnou součástí této Smlouvy je příloha:

   Příloha č. 1: Technická specifikace
   Příloha č. 2: Poptávkový list

V Praze dne: 15 -12- 2023

[redacted]

Jiří Dohnal
ra
Městská č[redacted]

[redacted]

Mgr. Ondřej Dedek
jednatel
Next Generation Security Solutions s.r.o.

Příloha č. 1 – Technická specifikace

	Technické požadavky	Splněno ANO /NE	popis řešení
1	Řešení musí v rámci licence podporovat zpracování 100 EPS (Event per second – událostí za sekundu)	ANO	Řešení IBM Security QRadar SIEM nabízí v základní licenci požadované množství EPS a budoucí rozšíření je možné.
2	Z celkového množství zpracovaných událostí musí být jejich část (především tedy události z kritické části infrastruktury) vyhodnocena interními pravidly a korelačními nástroji pro detekci kybernetických útoků vedoucí k tvorbě incidentů	ANO	Řešení IBM Security QRadar SIEM má věstavěný detekční engine, který pracuje s pravidly a vyhodnocuje příchozí logy skoro v reálném čase a generuje tak incidenty. Pomocí tohoto engine je možné out of the box ihned po instalaci detekovat pokročilé a složité kybernetické útoky.
3	Zbylá část zpracovaných událostí z ne kritických systémů bude pouze ukládána a dostupná pro budoucí analýzu. Počet takto ukládaných událostí, tedy tzv. ukládání bez pravidel a korelací, nesmí být co do počtu licenčně omezený, především z budoucího rozvoje a napojování dalších systému do SIEM řešení	ANO	Řešení IBM Security QRadar SIEM poskytuje možnost ukládání příchozích logů s příznakem "Log Only", tedy pouze uložení bez zapojení korelačního pravidlového systému. Takto označené příchozí události se licenčně nepočítají a neovlivňují EPS licenci (může jich být neomezené množství, záleží však na hardwarové kapacitě appliance, která logy zpracovává).
4	Řešení musí mít schopnost uchovat nejméně 45 TB dat (v komprimovaném formátu)	ANO	Řešení IBM Security QRadar SIEM není licenčně omezeno na velikost ukládaných dat a záleží pouze navrhnuté architektuře a jak velké uložiště má systém dostupné.
5	Řešení musí podporovat sběr událostí z prostředí Windows Server 2019+ a Linux	ANO	Řešení IBM Security QRadar SIEM podporuje sběr a zpracování logů z celé řady zařízení, včetně Windows a Linux strojů. Celkový seznam podporovaných zdrojů je možné najít v oficiální online dokumentaci zde https://www.ibm.com/docs/en/dsm?topic=configuration-qradar-supported-dsms
7	Řešení musí být dodáno jako softwarová instalace na virtuální servery	ANO	Řešení IBM Security QRadar SIEM je možné nasadit i v podobě virtuální appliance například nad platformou VMware vSphere.
8	Řešení musí podporovat minimálně tyto protokoly pro přijímání událostí: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE	ANO	Řešení IBM Security QRadar SIEM podporuje pro sběr logů všechny uvedené protokoly. Podporuje jak pasivní příjem logů, tak i aktivní vyčítání, např. z databází pomocí JDBC. Celkový seznam podporovaných protokolů pro sběr logů je možné najít v oficiální online dokumentaci zde https://www.ibm.com/docs/en/dsm?topic=configuration-protocol-options
9	Řešení musí umožňovat sběru logů lokálním kolektorem na off-site lokalitách s přeposíláním událostí do centrálního řešení, kde dochází k jejich vyhodnocení pravidly, případně se pouze uloží	ANO	Řešení IBM Security QRadar SIEM poskytuje více možností jak sbírat logy z off-site lokalit. První z nich je dedikovaný Event Collector appliance, který je spravován a součásti distribuivaného deploymentu a sbírá veškeré logy z offsite lokality. Druhou možností je Disconnected Log Collector (DLC), což je lightweight varianta Event Collector appliance s vetším lokálním bufferem.
10	Řešení musí podporovat možnost záložního uložení logů, tedy redundantní uložiště (rozšiřitelné úložiště neodpovídá tomuto požadavku)	ANO	Řešení IBM Security QRadar SIEM poskytuje záložní a archivační možnosti a jejich následné obnovení. Mimo to samozřejmě řešení IBM Security QRadar SIEM podporuje nasazení v modelu HA nebo DR.
11	Řešení poskytuje centrální moderní uživatelské rozhraní pro management všech komponent a administrativních funkcí a zároveň slouží mimo jiné pro nahlížení na sbírané události a k řešení detekovaných incidentů (analýza a reporting)	ANO	Řešení IBM Security QRadar SIEM nabízí centrální uživatelskou konzoli, odkud se nechá řídit celé nasazení a případná rozšíření.
12	Řešení musí umožňovat definovat uživatelům ALMu přístupová práva k jednotlivým funkcím, zařízením, reportům, skupinám, síťovým segmentům či jiným entitám, které nabízené řešení využívá	ANO	Řešení IBM Security QRadar SIEM používá uživatelské role a tzv. bezpečnostní profily, které řídí přístupová práva danému uživateli a definují to, co v rámci systému může dělat a které funkcionality může využívat.

13	Řešení musí podporovat rozpoznání a automatickou identifikaci nově připojeného systému (zdroje událostí)	ANO	Řešení IBM Security QRadar SIEM automaticky rozpoznává nový zdroj logů, přiřazuje korektní parser pro parsování logů a následně normalizuje a zpracovává příchozí logy.
14	Řešení musí podporovat šifrovanou komunikaci mezi zdroji logů a SIEM systémem (např. komunikace s log kolektorem)	ANO	Komunikace mezi komponenty řešení IBM Security QRadar SIEM může probíhat šifrovaně, tedy komunikace mezi Event Collectorem a centrální konzolí.
15	Řešení musí umožňovat integraci s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů	ANO	Řešení IBM Security QRadar SIEM poskytuje integraci jak na LDAP tak i na AD pro potřeby autentizace/autorizace uživatelů.
16	Řešení musí poskytovat jednoduché vizuální rozhraní pro správu zdrojů událostí (Log Source management). Toto rozhraní musí umožnit přidávat další zdroje událostí, přehledovou analýzu těch stávajících, nastavení parsovacích pravidel pro sbírané události a možnosti jejich archivování (nastavení různé délky životnosti ukládaných logů pro různé zdroje)	ANO	Řešení IBM Security QRadar SIEM nabízí moderní uživatelské rozhraní pro správu všech zdrojů logů, poskytující veškerou požadovanou funkcionalitu. Retenci dat pro různé zdroje logů je možné definovat pomocí takzvaných retenčních bucketů.
17	Řešení musí umožňovat manuální i automatické nastavené aktualizací systému	ANO	Řešení IBM Security QRadar SIEM nabízí automatické nebo manuální stahování parserů pro nerušený chod systému a kontinuální podporu zdroje logů.
18	Řešení musí poskytovat backup/recovery proces pro data a konfigurační nastavení, který pravidelně vytváří zálohy a v případě potřeby obnoví konfiguraci celého SIEM řešení (např. události, síťový tok, incidenty, konfigurace zdrojů logů, pravidla, reference sety, atd.)	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje.
19	Řešení musí poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému (řešení je schopno monitorovat samo sebe)	ANO	Řešení IBM Security QRadar SIEM ve výchozím stavu monitoruje sám sebe a veškeré prováděné konfigurační změny jsou auditovatelné. Administrátor nebo autorizovaný uživatel je upozorněn alertem v případě nějaké kritické situace.
20	Řešení musí poskytovat analytické a korelační funkce bez dalších zásahů a činností (out-of-the-box) pokrývající známé techniky a taktiky kybernetických útoků MITRE ATT&CK framework	ANO	Řešení IBM Security QRadar SIEM obsahuje hned po instalaci více než 350 korelačních bezpečnostních pravidel, které vedou k odhalení i těch nejpokročilejších kybernetických útoků. Pomocí aplikace Use Case Manager, QRadar SIEM mapuje všechna pravidla na MITRE ATT&CK framework a umožňuje jejich centrální správu.
21	Řešení musí být volně výkonově rozšiřitelné.	ANO	Řešení IBM Security QRadar SIEM podporuje z pohledu architektury takzvanou distribuovanou architekturu, kdy je možné systém horizontálně škálovat v závislosti na potřebách, výtíženosti a EPS (rozšíření může probíhat přidáním např. více Event Collectorů nebo Event Procesorů do deploymentu).
22	Popište, jak je nabízené řešení škálovatelné na požadavky: přidání nových zařízení (přidání nových zdrojů logů, tedy navýšení limitu EPS a nutnost přidat více zařízení pro jejich zpracování), lokací, aplikací atd.	ANO	Obdobně jak je popsáno v bodě výše. Řešení IBM Security QRadar SIEM lze škálovat horizontálně přídáním dalších appliance pro sběr nebo zpracování logů.
23	Řešení musí umožňovat modifikovat výběr (parsování) logů pomocí např. regulárních výrazů pro extrakci specifických atributů z obsahu logů	ANO	Řešení IBM Security QRadar SIEM poskytuje uživatelské rozhraní pro modifikaci out of the box parserů (DSM Editor) např. pro potřebu upravení parsování nebo zavedení Custom Event properties za pomoci využití regulárních výrazů nebo json.
24	Řešení musí zajišťovat integritu sbíraných dat, tedy integritu ukládaných logů např. pomocí file hashingu	ANO	Řešení IBM Security QRadar SIEM nabízí možnost file hashingu, tedy vytvoření hashe pro uložené událostí. Pomocí tohoto hashe je možné zpětně ověřit integritu uložených dat a zajistit to, že nebyly změněny.
25	Řešení musí poskytovat Near-real-time analýzu událostí	ANO	Součástí nabízeného řešení IBM Security QRadar SIEM je korelační engine, který pomocí pravidel vyhodnocuje příchozí události skoro v reálném čase a generuje tzv. Offenses.

26	Řešení poskytuje analýzu dlouhodobých trendů událostí	ANO	Výstupem řešení IBM Security QRadar SIEM je konsolidovaný incident/offense, který sjednocuje veškeré relevantní informace o daném kybernetickém útoku. Nejedná se o jednorázovou detekci, ale v případě déle trvajícího útoku nově příchozí události přispívají do již otevřeného offense a korelují se dohromady.
27	Řešení musí být hodnocené v segmentu „leaders" v Gartner Magic Quadrantu za minulé tři roky	ANO	Řešení IBM Security QRadar SIEM bylo a je v Leaders kvadrantu posledních 13 let.
28	Řešení musí poskytovat pokročilé analytické nástroje ("drill-down") pro prohledávání a analýzu sbíraných dat a pro rychlejší dohledání informací vedoucí k vyřešení kybernetického incidentu analytikem	ANO	Z přehledu všech aktivních Offense je možné se dostat na detail konkrétního Offense, kde jsou zachyceny veškeré relevantní informace včetně zdrojové IP adresy útoku, cílové destinace, relevatní logy a síťový tok, kategorizace, závažnost incidentu a další. Jednoduchým proklikem je možné zkoumat detailněji logy, případně síťový tok, a provádět tak prvotní triage incidentu.
29	Řešení musí umožňovat agregaci událostí z logů i podle položek které nejsou standardně zahrnuty v řešení (rozšiřitelnost na vlastně definované atributy např. pro reporting a auditing)	ANO	Podobně jak bylo již popsáno v bodu 23., řešení IBM Security QRadar SIEM poskytuje uživatelské rozhraní pro správu parserů, které mimochodem umožňuje definici vlastních normalizovaných polí a jejich naplnění vlastně definovaným regulárním výrazem (DSM editor). Takto vlastně definovaná pole se v rámci systému nazývají Custom Event Properties a pozdě je možné dle nich vyhledávat nebo případně tvořit pravidla a generovat reporty.
30	Řešení musí podporovat normalizaci časových značek z různých časových zón	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje.
31	Řešení musí podporovat sběr a zpracování logů z textových souborů	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje, viz bod 8. Celkový seznam podporovaných protokolů pro sběr logů je možné najít v oficiální online dokumentaci zde https://www.ibm.com/docs/en/dsm?topic=configuration-protocol-options
32	Řešení musí podporovat sběr logů z databází minimálně pomocí protokolů JDBC/ODBC	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje, viz bod 8. Celkový seznam podporovaných protokolů pro sběr logů je možné najít v oficiální online dokumentaci zde https://www.ibm.com/docs/en/dsm?topic=configuration-protocol-options
33	Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, Destination a Source IP adresa, typ události, protokol, port, samotný raw log jako takový atd.	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje a obsahuje celou řadu předpřipravených vyhledávacích dotazů, které je možné upravovat. Samozřejmostí je tvorba vlastních vyhledávacích dotazů a následná úprava sloupců, tedy rozložení zobrazovaných dat.
34	Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy případně pokročilejší operace typu WHERE, GROUP BY, HAVING, ORDER BY a další operace, známe například z databázového jazyk SQL, pro tvorbu složitějších vyhledávacích dotazů a reportů	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje pomocí proprietárního jazyka AQL, které syntaxí připomíná jazyk SQL a poskytuje nějaké funkce navíc pro bezpečnostní analytiky.
35	Řešení musí poskytovat alertování na detekované anomálie, změny chování sítě a změny v generování logů a událostí tvorbou incidentů obsahující detailní informace a odesláním emailu korektní osobu pro jejich vyřešení	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje.
36	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje. Možností alertingu nebo notifikací je více, například pomocí email, SMS, či jiné integrace na interně používané komunikační nástroje třetích stran. K notifikaci může dojít například po sepnutí některého z definovaných korelačních pravidel.
37	Řešení musí podporovat rozšíření o alerting, kdy dojde k porušení	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje. Možností alertingu nebo notifikací je více,

	definovaných bezpečnostních pravidel, založený na stanovené bezpečnostní politice		například pomocí email, SMS, či jiné integrace na interně používané komunikační nástroje třetích stran. K notifikaci může dojít například po sepnutí některého z definovaných korelačních pravidel.
38	Řešení musí umožňovat kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně	ANO	Řešení IBM Security QRadar SIEM umožňuje vyhledávat jak v indexovaných i neindexovaných datech buďto pomocí regulárních výrazů nebo fulltextového vyhledávání.
39	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a pokrývají z části techniky a taktiky známého MITRE ATT&CK frameworku	ANO	Řešení IBM Security QRadar SIEM obsahuje hned po instalaci více než 350 korelačních bezpečnostních pravidel, které vedou k odhalení i těch nejpokročilejších kybernetických útoků. Pomocí aplikace Use Case Manager, QRadar SIEM mapuje všechna pravidla na MITRE ATT&CK framework a umožňuje jejich centrální správu.
40	Řešení musí podporovat korelaci mezi zařízeními již po instalaci (out-of-the-box) bez nutné další konfigurace	ANO	Řešení IBM Security QRadar SIEM obsahuje hned po instalaci více než 350 korelačních bezpečnostních pravidel, které vedou k odhalení i těch nejpokročilejších kybernetických útoků. Pomocí aplikace Use Case Manager, QRadar SIEM mapuje všechna pravidla na MITRE ATT&CK framework a umožňuje jejich centrální správu.
41	Řešení musí podporovat vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje. V případě nutnosti je možné spustit tzv. Custom Action, což může být např. skript psaný v jazyce Python pro provedení nějaké složitější operace (např. přidání IP adresy na blacklist firewallu).
42	Řešení musí umožňovat pracovat s IP geolokacemi (botnet kanály atp.) a obohacovat artefakty (IP adresy, hashe souborů atd.) o zpravodajské informace z externích Threat Intelligence zdrojů	ANO	Součástí nabízeného řešení IBM Security QRadar SIEM je možnost využít IBM X-Force Threat Intelligence službu, která obohacuje artefakty v SIEM systému o aktuální zpravodajské informace.
43	Řešení musí být schopné odeslat alert o tom, že došlo k výpadku nějakého zdroje logů (přestal odesílat data do centrálního systému)	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu umožňuje, viz bod 36. a 37.
44	Řešení musí obsahovat mechanismus pro klasifikaci různých systémů podle jejich typu (např. mail, DHCP a DNS server atd.). Tuto klasifikaci aktiv lze následně využít během tvorby vlastních pravidel	ANO	Řešení IBM Security QRadar SIEM tuto funkcionalitu poskytuje v podobě tzv. Asset databáze, kde každý aktivní asset má vytvořený svůj vlastní profil, který mimo jiné obsahuje např. poslední IP adresu, MAC adresu, spojeného uživatele nebo seznam aktuálních zranitelností assetu a jeho zařazení do typu serverů. QRadar SIEM umožňuje tzv. Discovery & Classification, kdy na základě aktivit a logů z daného zdroje logů lze rozpoznat a označit, o jaký server se jedná (DNS, DHCP, databáze atd.). Tato klasifikace se následně nechá využívat v pravidlech.
45	Řešení musí podporovat schopnost monitorovat historii útoků (typů událostí) na kritické komponenty	ANO	Řešení IBM Security QRadar SIEM udržuje kompletní historie vzniklých Offenses a je možné provádět auditing.
46	Řešení musí podporovat schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele) v případě rozšíření o sledování síťových toků	ANO	Řešení IBM Security QRadar SIEM tuto funkcionality splňuje.
47	Řešení musí poskytovat rozhraní pro reporting. Mimo out-of-the-box reporty se od řešení očekává možnost tvorby vlastních, libovolně upravitelných reportů a jejich pravidelné spouštění	ANO	Řešení IBM Security QRadar SIEM tuto funkcionality splňuje a obsahuje hned po instalace desítky relevantních reportů, týkající se bezpečnosti organizace. Je možné tvořit vlastní reporty, především na základě uložených vyhledávacích dotazů.
48	Řešení musí podporovat nezměněnou funkcionalitu reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS	ANO	Nastavení reportingu není v nabízeném řešení IBM Security QRadar SIEM nijak spjato s konkretním zařízením nebo zdrojem dat. Vzhledem k tomu, že se pracuje s uloženými vyhledávacími dotazy v jazyce AQL, které pracují s normalizovanými eventy v systému, změna zdroje logů (např. změna firewallu) přímo neovlivní reporty. Logy z různých firewall jsou

			parsovány pomocí DSMs a výstupem je normalizovaná událost, např. Login Succesful. S touto normalizovanou událostí nadále systém pracuje dále ve vyhledávání a reportech.
49	Nabízené řešení musí poskytovat webové uživatelské rozhraní pro správu, analýzy, reportovaní a podobně. Rozhraní by nemělo obsahovat pluginy nebo být založeno na technologiích Java, Flash nebo na bázi tlustého klienta.	ANO	Řešení IBM Security QRadar SIEM nabízí centrální uživatelskou webovou konzoli, odkud se nechá řídit celé nasazení, konfigurace, vyhledávání, atd.
50	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.	ANO	Řešení IBM Security QRadar SIEM podporuje nasazení ve vysoké dostupnosti podobou active-standby clusteru s virtuální IP adresou, kterou sdílí obě appliances. Ať už se jedná o jakoukoliv komponentu, je možné ji nasadit v HA.
51	HA musí být možné nakonfigurovat a připojit v jakékoliv fázi projektu za běhu, bez nutnosti reinstalace celého řešení.	ANO	Nabízené řešení IBM Security QRadar SIEM podporuje konfiguraci vysoké dostupnosti kdykoliv, není nutná reinstalace prostředí.
52	Řešení musí poskytovat pravidelné aktualizace systému a jejich instalace by neměla omezit produkční provoz. Jejich instalace musí být natolik triviální, aby byla proveditelná bez zásahu profesionálních služeb dodavatele/výrobce	ANO	Ano, viz. bod 17. Řešení IBM Security QRadar SIEM rozlišuje aktualizace parserů, které mohou být automatické a probíhají skoro neustále. Vedle toho existují aktualizace systému samotného, kde release cycle podléhá modernímu přístupu Continuos Delivery a kvartálně jsou dostupné pro zákazníky nové minor verze produktu, které opravují otevřené problémy, bugy a dodávají do produktu novou funkcionalitu.
53	Některá zařízení v síti často mění svou IP adresu. Nabízené řešení musí být schopno udržet databázi zařízení konzistentní i v těchto případech. Popište, jak řešení splňuje tento požadavek.	ANO	Řešení IBM Security QRadar SIEM tento požadavek řeší pomocí tzv. Asset databáze a tvorbou Asset profilů pro každé aktivum pozorované na síti, viz. bod 44.
54	Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy a musí nabízet řádnou dokumentaci tohoto API	ANO	Nabízené řešení IBM Security QRadar SIEM poskytuje public REST API pro komunikaci a integraci s ostatními systémy, včetně dokumentace.
55	Řešení musí uchovávat logy jak v normalizovaném formátu, tak i v „raw" formátu.	ANO	Řešení IBM Security QRadar SIEM ukládá jak raw logy, tak normalizované události zpracované systémem.
56	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.	ANO	Řešení IBM Security QRadar SIEM není licenčně omezeno počtem korelačních pravidel.
57	Řešení musí být dodáno jako softwarová instalace na virtuální servery	ANO	Řešení IBM Security QRadar SIEM je možné nasadit i v podobě virtuální appliance například nad platformou VMware vSphere.
	Implementace a servis		
1	Instalace systému do infrastruktury zadavatele	ANO	10 člověkodnů – kvalifikovaného technika
2	Zaškolení	ANO	1 člověkoden – kvalifikovaného technika
3	3 hodiny práce kvalifikovaného technika měsíčně	ANO	Vzdáleným přístupem, na vyžádání v místě

	ÚMČ Praha 11 Odbor správy majetku	**POPTÁVKOVÝ LIST**	Výtisk č. 1

MĚSTSKÁ ČÁST PRAHA 11

se sídlem Ocelíkova 672, 149 41 Praha 4

Vám nabízí možnost předložit nabídku na zakázku malého rozsahu

dle §27 zákona č. 134/2016 Sb., o zadávání veřejných zakázek
ve znění pozdějších předpisů

OKT OI 20/2023
„Logmanager"

Zakázku lze zadat zájemci, který splní tyto předběžné požadavky a podmínky:

1. Předmět plnění zakázky

Předmětem zakázky je dodávka centralizovaného ukládání a správa logů z libovolných zdrojů, s možností analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací formou služby na 12 měsíců.

Obecný popis:

Dodat a implementovat centrální úložiště pro sběr a analýzu logů (SEM řešení) s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, zejména pak doložením souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpět. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi pro vytváření reportů.

Technická kvalifikace

Účastníci prokáží technickou kvalifikaci předložením:

1. Seznamu 2 významných služeb s obdobným předmětem plnění jako je předmět veřejné zakázky, tj. zajištění log managementu v segmentu státní správy nebo územní samosprávy, o finančním objemu každé z nich větším než 400.000 Kč bez DPH poskytnutých dodavatelem za poslední 3 roky před zahájením zadávacího řízení. V předloženém seznamu bude uvedena

identifikace objednatele, názvu významné dodávky, popisu významné dodávky, ceny a doby poskytnutí významné dodávky a kontaktní osoby objednatele.

2. Osvědčení o vzdělání a odborné kvalifikaci účastníka nebo vedoucích zaměstnanců účastníka nebo osob v obdobném postavení a osob odpovědných za vedení realizace příslušných stavebních prací.

Bezpečnostní architekt

Minimální úroveň:

i. Praxe v oboru na pozici bezpečnostní architekt min. 4 roky.

ii. Předložením související mezinárodní certifikace z oblasti bezpečnosti IT: CISA, CISM, CISSP, ISO/IEC 27001, ISMS Lead Auditor apod. Postačující je předložení alespoň jednoho z uvedených certifikátů.

Způsob prokázání kvalifikace:

i. Doklad o dokončeném vzdělání

ii. Certifikace člena týmu

iii. Životopis člena týmu včetně čestného prohlášení osoby o délce praxe

Specialista log managementu

Minimální úroveň:

i. Ukončené středoškolské nebo vysokoškolské vzdělání

ii. Praxe v oboru na pozici specialista log managementu min. 2 roky

iii. Certifikace výrobce dodávané technologie

Způsob prokázání kvalifikace:

i. Doklad o dokončeném vzdělání

ii. Certifikace člena týmu

iii. Životopis člena týmu včetně čestného prohlášení osoby o délce praxe

Technické požadavky řešení - v příloze - technická specifikace.xlsx

2. Nabídková cena

Nabídková cena musí být cenou obvyklou v místě plnění a je nutno ji zpracovat v následujícím členění:

- cena bez DPH
- výše DPH v % a částka DPH v Kč
- cena celkem (tj. včetně DPH)

Výše uvedené ceny platí pro místo plnění zakázky, kterým je Praha 11.

3. Platební podmínky

- lhůty splatnosti faktur 21 dnů od doručení
- záloha nebude poskytnuta

4. Doba plnění:

Termín předání předmětu plnění je nejpozději 31.12.2023, užití služby na 12 měsíců od předání.

5. Návrh smlouvy/objednávka

Na předmět díla bude uzavřena smlouva předložená uchazečem. Návrh smlouvy o dílo musí obsahovat následující ustanovení a musí být podepsán oprávněnou osobou:

Závěrečná ustanovení

- Tato smlouva nabývá účinnosti dnem uveřejnění prostřednictvím registr smluv.
- Smluvní strany se dohodly, že tato smlouva je veřejně přístupnou listinou podle zákona č. 106/1999 Sb., ve znění pozdějších předpisů.
- Smlouva je provedena v pěti vyhotoveních, zadavatel obdrží tři vyhotovení a dodavatel dvě vyhotovení.
- Doložka dle zákona o hl. m. Praze: uzavření této smlouvy schválila RMČ usnesením č. XXXX/YY/R/2023 ze dne DD.MM.2023 a k jeho podpisu je pověřena Jiří Dohnal, radní MČ Praha 11, na základě usnesení RMČ č. XXXX/YY/R/2023 ze dne DD.MM.2023.

6. Způsob hodnocení nabídek a kritéria hodnocení nabídek

Předložené nabídky budou hodnoceny s přihlédnutím k ekonomické výhodnosti dle následujících kritérií:

- nabídková cena 100 %

7. Minimální kvalifikační předpoklady, závazné podstatné náležitosti nabídky, a jiná ujednání

7.1. Zadavatel požaduje prokázat základní způsobilost zájemce, prokazující, že uchazeč

a) nebyl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 zákona č. 134/2016 Sb. o zadávání veřejných zakázek nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,

b) nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,

c) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,

d) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,

e) není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla vůči němu nařízena nucená správa nebo není v obdobné situaci podle právního řádu země sídla dodavatele.

Splnění výše uvedených požadavků na základní způsobilost uchazeč prokáže předložením čestného prohlášení. Z obsahu čestného prohlášení musí být zřejmé, že uchazeč splňuje příslušnou základní způsobilost požadovanou zadavatelem. Je-li dodavatelem právnická osoba, musí z čestného prohlášení být zřejmé, že podmínku podle písm. a) tohoto článku splňuje tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí z čestného prohlášení být zřejmé, že podmínku podle písm. a) tohoto článku splňuje tato právnická osoba, každý člen statutárního orgánu této právnické osoby a osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

7.2. Zadavatel požaduje prokázat profesní způsobilost uchazeče předložením:

- výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje
- dokladu, že je oprávněn podnikat v rozsahu odpovídajícímu předmětu veřejné zakázky, pokud jiné právní předpisy takové oprávnění vyžadují
- dokladu, že je odborně způsobilý nebo disponuje osobou, jejímž prostřednictvím odbornou způsobilost zabezpečuje, je-li pro plnění veřejné zakázky odborná způsobilost jinými právními předpisy vyžadována.

Doklady prokazující profesní způsobilost musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem uplynutí lhůty pro podání nabídek. Veškeré doklady vyjma čestných prohlášení přikládá zájemce v prosté kopii.

Veškeré doklady k prokázání technické kvalifikace dokládá uchazeč v prosté kopii.

V případě, že uchazeč není schopen prokázat splnění určité části profesní způsobilosti nebo technické kvalifikace požadované zadavatelem k plnění veřejné zakázky v plném rozsahu, je oprávněn splnění kvalifikace v chybějícím rozsahu prokázat prostřednictvím jiných osob. Uchazeč v takovém případě doloží:

- doklady prokazující splnění základní a profesní způsobilosti jinou osobou
- doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,

- písemný závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude uchazeč oprávněn disponovat v rámci plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele

7.3. Součástí nabídky dále bude:

- platný kontaktní email a telefonní číslo uchazeče
- prohlášení uchazeče, že uchazeč podáním své nabídky v rámci této veřejné zakázky souhlasí s uveřejněním své nabídky na webových stránkách MČ Praha 11 z důvodu maximálního naplnění zásady transparentnosti
    - kompletní elektronická verze nabídky bude v elektronické podobě ve formátu doc, docx, ,xls, xlsx, pdf

7.4. Uchazeč prokáže splnění technické kvalifikace předložením seznamu služeb/dodávek spočívajících v realizaci minimálně tří zakázek obdobného charakteru a finančního objemu, realizovaných za poslední 3 roky před zahájením zadávacího řízení.

8. Lhůta a místo pro podání nabídek

Nabídku musí uchazeč doručit nejpozději do 12:00 hodin dne 06-12-2023 do podatelny Úřadu městské části Praha 11, Ocelíkova 672, 149 41 Praha 4.

Přední strana obálky s nabídkou musí být označena takto:

NEOTVÍRAT
ZAKÁZKA

„Logmanager"

Zadní strana nabídky musí obsahovat identifikaci účastníka

9. Zadávací lhůta

Uchazeči jsou svými nabídkami vázáni po dobu 60 kalendářních dnů, která začíná běžet dne ....., tj. následující den po skončení lhůty podání nabídek.

07-12-2023

10. Osoba oprávněná jednat za zadavatele a sdělení informací

Ing. Miroslav Zábranský
vedoucí Odboru správy majetku
ÚMČ Praha 11
tel.: [redacted]
e-mail: [redacted]

12. Práva zadavatele

Zadavatel si vyhrazuje právo zrušit zakázku do podpisu smlouvy

Zadavatel si vyhrazuje právo měnit nebo doplnit další požadavky této výzvy shodně pro všechny uchazeče před uplynutím lhůty pro podání nabídek

13. Závěrečná ustanovení

Na základě interních předpisů zadavatele výkon zadavatelských činností provádí Odbor správy majetku ÚMČ Praha 11.
Přílohy:

- krycí list nabídky
- technická specifikace.xlsx
- vzor čestného prohlášení

Praha 21 -11- 2023

za zadavatele

[redacted]

Jiří Dohnal
radní MČ Praha 11