PŘÍLOHA Č. 1

Specifikace Dodávky

Požadavky Objednatele

Předmětem této veřejné zakázky je rozšíření stávající platformy SIEM (Security Information and Event Managment), který je v prostředí MHMP implementována jako platforma pro sběr, detekci a vyhodnocování bezpečnostních událostí.

Součástí dodávky bude doplnění potřebných licencí, implementace a technická podpora systémového řešení, včetně podpory bezpečnostního týmu zadavatele po dobu 3 let, pro zajištění účinné detekce a následného zvládnutí pokročilých kybernetických útoků vedených na informační aktiva systémů MPHMP.

Řešení bude pomáhat naplňovat požadavek na detekci bezpečnostní události a následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 zákona č. 181/2014 sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů a požadavky obecného nařízení (EU) 2016/679 (GDPR).

Dodávané řešení spolu s podporou výrobce a dodavatele na 3 roky zaručí vysokou bezpečnost organizace pro toto období.

Z důvodu požadovaného rozšíření systému SIEM pro potřeby MPHMP je požadována dodávka software, implementace a následné podpory takto:

a) Dodávka rozšíření licencí SIEM, včetně 3 leté subskripce nových verzí a aktualizací
b) Instalace, implementace a školení
c) Záruka za jakost a servisní podpora

A. Požadované detailní parametry rozšíření licencí SIEM

Zadavatel v současnosti provozuje řešení postavené na následujících softwarových komponentách a požaduje jejich rozšíření, včetně 3 leté produktové podpory a nároku na aktualizace.

- SQM IBM Security QRadar SIEM
- SQM IBM Security QRadar Vulnerability Manager
- IBM Resilient Incident Response Platform (PA)
- SQM IBM Security Guardium Data Protection for Databases
- SQM IBM Security Guardium Vulnerability Assessment for Databases
- SQM IBM BigFix Lifecycle Client Device License
- SQM IBM BigFix Lifecycle Managed Virtual Server

Platforma SQM využívá veškerou funkcionalitu licencích IBM a doplňuje ji o profesionální správu celé SIEM platformy, prvky vlastního dohledového systému a služby bezpečnostního monitoringu s vyhodnocováním bezpečnostních incidentů v dohledovém centru

poskytovatele. Díky unikátním systému vlastního monitoringu a služeb vícestupňové analytické podpory, tak umožňuje řešení nejen efektivně reagovat na již proběhlé bezpečnostní incidenty, ale dokonce tyto incidenty předvídat, vyšetřovat a předcházet jim.

Řešení poskytuje nejen standardní log management, event management, reporting a analýzy chování pro sítě a aplikace nebo uživatele, ale i nejmodernější funkcionalitu v podobě komplexního chápání různých zdrojů a relevantních bezpečnostních informací. Společně s doplňujícími moduly pro rozšíření funkcionality a zpřesnění detekce jakou jsou Management zranitelnost, pro efektivní práci a korelaci zranitelností či Management rizik, umožní tvorbu "Co – Když" analýz a v neposlední řadě také s modulem forenzního řízení a řešení bezpečnostních incidentů, doplněný o služby bezpečnostního monitoringu a analytiků ve všech fázích – od detekce potenciálních slabých míst, detekci a následné investigaci chování. Řešení je dále obohaceno o moduly ochrany databází a souborů či ochranu koncových bodů.

Požadavky na rozšíření stávajících licencí:

Modul	Detailní požadavek	Požadavek navýšení	Nabídka uchazeče
QSM Qradar	QRadar Software Node	+ 4 licence	+ 4 licence
QSM Qradar	Flows Capacity, Flows Per Minute License	+ 150000 flows	+ 150000 flows
QSM Qradar	Vulnerability Manager Capacity	+ 512 assets	+ 512 assets
Resilient	Incident Response Platform Standard Authorized User License	+ 2 uživatele	+ 2 uživatele
QSM Guardium	Security Guardium Data Protection for Databases Resource Value Unit	+ 9 licencí	+ 9 licencí
QSM Guardium	Security Guardium Collector Software Appliance Install License	+ 2 licence	+ 2 licence
QSM Big-Fix	IBM BigFix Lifecycle Managed Virtual Server Lic	+ 190 serverů	+ 190 serverů

Nabídka rozšíření je požadována, včetně 3 leté produktové podpory a nároku na aktualizace.

B. Požadavky na instalaci, implementaci a školení

Dodavatele provede samostatně instalaci a zapojení v místě plnění. Součástí implementace je dodávka Detailního návrhu řešení a zaškolení. Předpokládaný minimální rozsah implementace je 120 člověkodnů.

Detailního návrhu řešení. Dodavatel se seznámí s architekturou počítačové sítě objednatele. Výstupem této analýzy bude Detailní návrh řešení, který bude obsahovat:

- způsob zasílání logů do řešení SIEM minimálně z 10 zdrojů typu: síťové přepínače, servery Windows, servery Linux, databáze, poštovní systém Exchange, antispam, antivirus, monitorovací síťové řešení, IPS/IDS, aplikační firewall, disková pole, servery;
- způsob iniciálního nastavení alarmů, reportů, rolí a uživatelů;
- doporučení činnosti k provozování a údržbě řešení SIEM kupujícím.

Detailní návrh bude podroben interní oponentuře Objednatele. V případě připomínek Objednatele je Dodavatel povinen tyto připomínky do detailního návrhu řešení zapracovat. Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky.

Implementace

Implementace SIEM do prostředí Objednatele začne na základě akceptovaného a předaného Detailního návrhu řešení.

S ohledem na velký počet informačních systému budou v první řadě identifikovány a realizovány tři (3) významné informační systémy a poté deset (10) typů společné síťové infrastruktury, neurčí-li pořadí a rozsah Objednatelem akceptovaný Detailní návrh řešení jinak.

Objednatel požaduje v rámci implementace integrovat a podrobně zdokumentovat 10 typů zdrojů logů a událostí do systému SIEM. Nativní nebo v rámci dodávky integrovaná podpora aplikací (sběr dat, parsování a jejich normalizace) musí být Dodavatelem poskytnuta na klíč.

Min. výčet typů zdrojů pro integraci jsou tyto zdroje: síťové přepínače, servery Windows, servery Linux, databáze, poštovní systém Exchange, antispam, antivirus, monitorovací síťové řešení, IPS/IDS, aplikační firewall, disková pole a servery

Následně po zapojení těchto informačních systémů do bezpečnostního monitoringu budou v rámci rutinního provozu vybrány další logsource tj. informační systémy z identifikovaných kritických aplikací, z pohledu bezpečnosti, a ostatní zdroje, které budou potupně napojovány na bezpečnostní monitoring v rámci služby základní a rozšířené podpora SIEM.

Požadavky na implementaci díla

Součástí předmětu plnění je:

- dodání potřebného programového vybavení (SW) a jeho instalace v datových centrech objednatele
  - Objednatel poskytne vlastní HW prostředky
  - Objednatel alternativně poskytne virtuální prostředí, včetně licencí, pro zprovoznění požadovaných licencí (virtualizace na platformě VMware);

Instalace a základní konfigurace systému SIEM:

- instalace a uvedení do provozu všech komponent,
- nastavení kompletní vzájemné komunikace komponent,
- aktualizace všech komponent na poslední podporované verze,
- nastavení automatických aktualizací,
- konfigurace zálohování a archivace na prostředky přidělené Objednatelem;

Integrace monitorovaných technologií:

- nastavení sběru událostí ze všech monitorovaných technologií,
- nastavení zpracování událostí ze všech monitorovaných technologií,
- vytvoření logických skupin monitorovaných zařízení podle typu;

Konfigurace přístupů:

- konfigurace rolí/skupin,
- nastavení oprávnění k monitorovaným zdrojům dle kompetencí;

Testování a ověření funkčnosti:

- otestování sběru událostí ze všech monitorovaných zařízení,
- otestování správné funkce korelačních pravidel,
- otestování správného generování a obsahu alertů a reportů,
- otestování oprávnění;

Zpracování dokumentace v rozsahu:

- popis řešení a jeho jednotlivých komponent,
- výčet použitých HW komponent včetně výrobních čísel,
- výčet použitých SW licencí,
- technická specifikace,
- provozní dokumentace.

Výčet typů zařízení MPHMP pro implementaci:

Zařízení / Druh	Množství
Windows Active Directory Servers	2
Windows IIS and Exchange Servers	54
Windows General Purpose Servers	18
UNIX and Linux Servers	41
DNS / DHCP Servers	3
Antivirus Servers	1
Database Servers	9
Proxy Servers	2
Large Firewalls	2
Small Firewalls	45

IDS, IPS and DAM	2
VPN	45
Routers and Switches	190
zOS DB2	2
Application Server	56
RADIUS / LDAP	4
Load Balancers	2
Email Content/Spam Filtering	1
Total Workstations on Network	770
Total Servers on Network	190

V rámci implementace bude provedena konfigurace pro 10 typů zařízení a to způsobem, který Dodavatel navrhne v Detailním návrhu řešení a Objednatel stvrdí akceptací.

Školení

Předmětem veřejné zakázky je rovněž provedení školení pro uživatele a administrátory Objednatele k používání a správě SIEM. Školení 2 administrátorů SIEM v celkovém rozsahu 16 hodin. Školení musí proběhnout v sídle Objednatele, a to nejpozději před akceptací díla. Za organizační zajištění školení zodpovídá dodavatel. Objednatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti.

C. Požadavky na záruku za jakost a servisní podporu

Záruka za jakost a s tím spojená **podpora** je požadována na 36 měsíců od akceptace předmětné části plnění

Podpora řešení SIEM na 36 měsíců zahájí okamžikem podpisu smlouvy a spočívá v poskytování servisní a poradenská podpory provozu řešení SIEM, při řešení provozních problémů a vyhodnocování událostí v minimálním rozsahu 216 člověkodnů za 36 měsíců, tj. minimálně 6 člověkodnů měsíčně, takto:

Služby údržby SIEM – maintenance – v rozsahu 1 MD měsíčně

- Poskytování nových verzí SIEM a opravných patchů
- Poskytování služeb monitoringu a dohledových služeb nad platformou SIEM, tj. zaručený provoz, v režimu 24/7/365, monitoringu nad dodaným HW/SW řešením.

Služby základní a rozšířené podpory SIEM – v rozsahu 5 MD měsíčně

- Poskytování služby HotLine/Helpdesk, včetně servisní technické podpory SIEM
- Poskytování poradenských služeb certifikovaným bezpečnostním konzultantem prostřednictvím HotLine/Helpdesk při řešení běžných

provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.

- Poskytování služeb bezpečnostního monitoringu (24/7/365), prostřednictvím vyhodnocovacího centra pro řešení incidentů, a to denně v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.
- Služby přidávání dalších logsource a vyhodnocování bezpečnostních událostí, dle požadavků
- Vyhodnocení bezpečnostních událostí převedení v bezpečnostní incidenty s relevantním hodnocením kritičnosti - omezeno počtem 8 popsaných incidentů měsíčně.
- Školení dle požadavků Objednatele nad sjednaný rozsah.
- Součinnost při řešení implementaci systémů třetích stran.
- Úpravy a funkční doplnění SIEM dle požadavků Objednatele.

Dodavatel se zavazuje, že veškeré plnění (analýza, implementace, vyhodnocení pilotního provozu i následná podpora dodávaného SIEM řešení) provedou pracovníci s odpovídající kvalifikací, kteří jsou výrobcem dodávaného systému SIEM certifikováni k provádění technické podpory dodávaných technických i programových prostředků.

Místo plnění

Místem plnění je:

1) Datové centrum Magistrátu hl. m. Prahy, v lokalitě Praha 4 – Chodovec
2) Datové centrum Městské Policie Hl. m. Prahy, v lokalitě Praha 10 - Korunní

Nabízené řešení Dodavatelem

TOTAL SERVICE a.s. doplní potřebný počet licencí, zajistí implementaci a technickou podporu systémového řešení, včetně podpory bezpečnostního týmu zadavatele po dobu 3 let, pro zajištění účinné detekce a následného zvládnutí pokročilých kybernetických útoků vedených na informační aktiva systémů MPHMP.

Součástí plnění bude dodávka software, implementace a následné podpory takto:

a) Dodávka rozšíření licencí SIEM, včetně 3 leté subskripce nových verzí a aktualizací
b) Instalace, implementace a školení
c) Záruka za jakost a servisní podpora

Seznam poskytnutých licencí, včetně 36 měsíců podpory

KS	POPIS LICENCE
4	QSM IBM **QRADAR SOFTWARE NODE** INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
1	QSM IBM QRADAR **FLOWS CAPACITY 100K** FLOWS PER MINUTE LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
1	QSM IBM QRADAR **FLOWS CAPACITY 50K** FLOWS PER MINUTE LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
1	QSM IBM SECURITY QRADAR **VULNERABILITY MANAGER** CAPACITY INCREASE 512 INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
2	IBM **RESILIENT** INCIDENT RESPONSE PLATFORM STANDARD AUTHORIZED USER LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
9	QSM IBM SECURITY **GUARDIUM DATA PROTECTION** FOR DATABASES RESOURCE VALUE UNIT (MVS) LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
2	QSM IBM SECURITY **GUARDIUM COLLECTOR** SOFTWARE APPLIANCE INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 36 MONTHS
190	QSM IBM **BIGFIX LIFECYCLE** MANAGED VIRTUAL SERVER LIC + SW S&S 36 MONTHS

Rozšíření licencí SIEM

TOTAL SERVICE a.s. dodá rozšíření instalované báze produktu v 100% shodě s požadavky zadávací dokumentace takto:

Modul	Detailní požadavek	Požadavek navýšení	Nabídka uchazeče
QSM Qradar	QRadar Software Node	+ 4 licence	+ 4 licence
QSM Qradar	Flows Capacity, Flows Per Minute License	+ 150000 flows	+ 150000 flows
QSM Qradar	Vulnerability Manager Capacity	+ 512 assets	+ 512 assets
Resilient	Incident Response Platform Standard Authorized User License	+ 2 uživatele	+ 2 uživatele
QSM Guardium	Security Guardium Data Protection for Databases Resource Value Unit	+ 9 licencí	+ 9 licencí
QSM Guardium	Security Guardium Collector Software Appliance Install License	+ 2 licence	+ 2 licence
QSM Big-Fix	IBM BigFix Lifecycle Managed Virtual Server Lic	+ 190 serverů	+ 190 serverů

Licence budou dodány včetně 3 leté produktové podpory a nároku na aktualizace.

Dodávka instalace, implementace a školení

Dodavatele provede samostatně instalaci a zapojení v místě plnění. Součástí implementace bude dodávka Detailního návrhu řešení a zaškolení.

Nabízený rozsah implementace je **120 člověkodnů**.

TOTAL SERVICE a.s. se seznámí s architekturou počítačové sítě objednatele. Výstupem této analýzy bude Detailní návrh řešení, který bude obsahovat:

- způsob zasílání logů do řešení SIEM minimálně z 10 zdrojů typu: síťové přepínače, servery Windows, servery Linux, databáze, poštovní systém Exchange, antispam, antivirus, monitorovací síťové řešení, IPS/IDS, aplikační firewall, disková pole, servery;
- způsob iniciálního nastavení alarmů, reportů, rolí a uživatelů;
- doporučení činnosti k provozování a údržbě řešení SIEM kupujícím.

Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky.

Implementace

Implementace SIEM do prostředí Objednatele začne na základě akceptovaného a předaného Detailního návrhu řešení.

S ohledem na velký počet informačních systému budou v první řadě identifikovány a realizovány tři (3) významné informační systémy a poté deset (10) typů společné síťové infrastruktury, neurčí-li pořadí a rozsah Objednatelem akceptovaný Detailní návrh řešení jinak.

Servery budou instalovány do virtuálního prostředí Zadavatele na platformě VMware, celkový potřebný počet VM serverů bude určen v Detailním návrhu řešení.

Součástí předmětu plnění je:

- dodání potřebného programového vybavení (SW) a jeho instalace v datových centrech objednatele
  - Objednatel poskytne vlastní HW prostředky
  - Objednatel alternativně poskytne virtuální prostředí, včetně licencí, pro zprovoznění požadovaných licencí (virtualizace na platformě VMware);

Instalace a základní konfigurace systému SIEM:

- instalace a uvedení do provozu všech komponent,
- nastavení kompletní vzájemné komunikace komponent,
- aktualizace všech komponent na poslední podporované verze,
- nastavení automatických aktualizací,
- konfigurace zálohování a archivace na prostředky přidělené Objednatelem;

Integrace monitorovaných technologií:

- nastavení sběru událostí ze všech monitorovaných technologií,

- nastavení zpracování událostí ze všech monitorovaných technologií,
- vytvoření logických skupin monitorovaných zařízení podle typu;

Konfigurace přístupů:

- konfigurace rolí/skupin,
- nastavení oprávnění k monitorovaným zdrojům dle kompetencí;

Testování a ověření funkčnosti:

- otestování sběru událostí ze všech monitorovaných zařízení,
- otestování správné funkce korelačních pravidel,
- otestování správného generování a obsahu alertů a reportů,
- otestování oprávnění;

Zpracování dokumentace v rozsahu:

- popis řešení a jeho jednotlivých komponent,
- výčet použitých HW komponent včetně výrobních čísel,
- výčet použitých SW licencí,
- technická specifikace,
- provozní dokumentace.

Výčet typů zařízení MPHMP pro implementaci:

Zařízení / Druh	Množství
Windows Active Directory Servers	2
Windows IIS and Exchange Servers	54
Windows General Purpose Servers	18
UNIX and Linux Servers	41
DNS / DHCP Servers	3
Antivirus Servers	1
Database Servers	9
Proxy Servers	2
Large Firewalls	2
Small Firewalls	45
IDS, IPS and DAM	2
VPN	45
Routers and Switches	190
zOS DB2	2
Application Server	56
RADIUS / LDAP	4
Load Balancers	2
Email Content/Spam Filtering	1
Total Workstations on Network	770
Total Servers on Network	190

V rámci implementace bude provedena konfigurace pro 10 typů zařízení a to způsobem, který Dodavatel navrhne v Detailním návrhu řešení a Objednatel stvrdí akceptací.

Školení

Předmětem dodávky TOTAL SERVICE a.s. je rovněž provedení školení pro uživatele a administrátory Objednatele k používání a správě SIEM. Školení 2 administrátorů SIEM v celkovém rozsahu 16 hodin. Školení musí proběhnout v sídle Objednatele, a to nejpozději před akceptací díla. Za organizační zajištění školení zodpovídá dodavatel. Objednatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti.

Záruka za jakost a servisní podporu

Záruka za jakost a s tím spojená **podpora** bude poskytnuta na 36 měsíců od akceptace předmětné části plnění.

Podpora řešení SIEM na 36 měsíců zahájí okamžikem podpisu smlouvy a spočívá v poskytování servisní a poradenská podpory provozu řešení SIEM, při řešení provozních problémů a vyhodnocování událostí v minimálním rozsahu 216 člověkodnů za 36 měsíců, tj. 6 člověkodnů měsíčně, takto:

Služby údržby SIEM – maintenance – v rozsahu 1 MD měsíčně

- Poskytování nových verzí SIEM a opravných patchů
- Poskytování služeb monitoringu a dohledových služeb nad platformou SIEM, tj. zaručený provoz, v režimu 24/7/365, monitoringu nad dodaným HW/SW řešením.

Služby základní a rozšířené podpory SIEM – v rozsahu 5 MD měsíčně

- Poskytování služby HotLine/Helpdesk, včetně servisní technické podpory SIEM
- Poskytování poradenských služeb certifikovaným bezpečnostním konzultantem prostřednictvím HotLine/Helpdesk při řešení běžných provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.
- Poskytování služeb bezpečnostního monitoringu (24/7/365), prostřednictvím vyhodnocovacího centra pro řešení incidentů, a to denně v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.
- Služby přidávání dalších logsource a vyhodnocování bezpečnostních událostí, dle požadavků
- Vyhodnocení bezpečnostních událostí převedení v bezpečnostní incidenty s relevantním hodnocením kritičnosti - omezeno počtem 8 popsaných incidentů měsíčně.
- Školení dle požadavků Objednatele nad sjednaný rozsah.
- Součinnost při řešení implementaci systémů třetích stran.
- Úpravy a funkční doplnění SIEM dle požadavků Objednatele.

TOTAL SERVICE a.s. se zavazuje, že veškeré plnění (analýza, implementace, vyhodnocení pilotního provozu i následná podpora dodávaného SIEM řešení) provedou pracovníci s odpovídající kvalifikací, kteří jsou výrobcem dodávaného systému SIEM certifikováni k provádění technické podpory dodávaných technických i programových prostředků.

Místo plnění

Místem plnění je:

1) Datové centrum Magistrátu hl. m. Prahy, v lokalitě Praha 4 – Chodovec
2) Datové centrum Městské Policie Hl. m. Prahy, v lokalitě Praha 10 - Korunní