Aktualizované znění dle dodatečných informací k zadávacím podmínkám č. 1

ZADÁVACÍ DOKUMENTACE

dle § 44 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů
(dále jen „ZVZ“),

k nadlimitní veřejné zakázce na dodávky zadávané v otevřeném řízení
dle § 21 odst. 1 písm. a) a § 27 ZVZ

s názvem

„SIEM – rozvoj zabezpečení rezortní sítě“

(dále jen „veřejná zakázka“)

1. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE:

Název:	Česká republika – Ministerstvo životního prostředí
Sídlo:	Vršovická 1442/65, 100 10, Praha 10
IČO:	00164801/není plátcem DPH
Bankovní spojení:	ČNB Praha 1
Číslo účtu:	000000-7628001/0710
Jednající:	Ing. Janou Vodičkovou
	ředitelkou odboru informatiky
Kontaktní osoba:	Ing. David Špalt, vedoucí oddělení informatiky
E-mail:	David.Spalt@mzp.cz
Telefon:	267 122 947
Kontaktní osoba:	Mgr. Kateřina Hochová, samostatné oddělení veřejných zakázek
E-mail:	Katerina.Hochova@mzp.cz
Telefon:	267 122 386

(dále jen „zadavatel“)

2. PŘEDMĚT VEŘEJNÉ ZAKÁZKY

2.1 Předmět veřejné zakázky

Předmětem veřejné zakázky je rozvoj stávajícího Security Information and Event Management (dále také „SIEM“) Ministerstva životního prostředí (dále také „MŽP“) a implementace proaktivních zdrojů NetFlow, a to včetně podpory po dobu tří (3) let.

Hlavním cílem veřejné zakázky je:

- Detekovat síťové útoky v rámci celé infrastruktury - nejen v rámci sítě MŽP;
- Detekovat pokročilé útoky jako jsou APT apod.;
- Předcházet potencionálním útokům díky znalosti slabých míst (zranitelností) a znalosti možných dopadů potencionálních útoků;
- Schopnost přesně určit povahu hrozeb a aktivně před nimi chránit infrastrukturu;
- Efektivně vyhodnocovat incidenty se správnou prioritou.

V rámci předmětu plnění zadavatel poptává:

A. Dodávku komponent:

- Skener zranitelností pro odhalování zranitelností v infrastruktuře;
- Samostatnou NetFlow sondu pro sběr síťového provozu;
- Samostatný NetFlow kolektor pro sběr a vyhodnocování NetFlow;

- Modul detekce anomálií na sítí (NBA);
- UTM (Unified Thread Management) - zařízení, které v sobě integruje firewall, VPN (IPSec, SSL), IDS/IPS, antivirus, antispyware, antispam, filtrování webového obsahu, aplikační filtraci, QoS.

Vítězný uchazeč je povinen při dodání výše specifikovaných komponent předložit zadavateli platnou registraci podpory u jednotlivých komponent na dobu tří (3) let.

B. Projektové práce:

- Projekt implementace a integrace všech komponent a dalších systémů MŽP do stávajícího řešení SIEM v rámci stávajícího konceptu bezpečnostního monitoringu:
  - Integrace NetFlow sondy s NetFlow kolektorem;
  - Integrace NetFlow sondy s QRadarem;
  - Integrace NetFlow kolektoru s modulem detekce anomálií (NBA);
  - Integrace modulu detekce anomálií (NBA) pomocí protokolu syslog a SNMP do QRadar SIEM;
  - Vytvoření konektoru a přidání nových pravidel pro vyhodnocování událostí z modulu anomálií (NBA);
  - Nastavení modulu detekce anomálií (NBA) a prvotní odladění false positive;
  - Nastavení UTM a prvotní odladění false positive;
  - Integraci UTM do QRadar a vytvoření či úprava pravidel.
- Předvedení funkčnosti implementovaného řešení a seznámení administrátorů SIEM MŽP s monitoringem síťového provozu v souvislosti s novými zdroji NetFlow.

Projektové práce jsou předpokládány v maximálním rozsahu patnácti (15) člověkodnů s tím, že cena za Projektové práce bude uhrazena dle skutečného čerpání a sazby za člověkoden (nejvýše však v rozsahu 15 člověkodnů).

C. Servisní podporu komponent:

Pro veškeré rozšiřující komponenty (HW, SW) požaduje zadavatel podporu na dobu tří (3) let, přičemž podpora bude zahrnovat:

- Nové upgrades a updates – vítězný uchazeč bude muset informovat zadavatele a tyto mu zpřístupnit do 20 pracovních dnů od jejich vydání. Upgrade bude proveden zadavatelem svépomocí s případným využitím konzultací vítězného uchazeče.
- Patche a opravy chyb – vítězný uchazeč bude muset informovat a zpřístupnit zadavateli vydání patche opravující závažné bezpečnostní nebo funkční chyby softwaru – doba nahlášení bude činit 5 pracovních dní od vydání patche. Implementaci patche provede zadavatel svépomocí s případným využitím konzultací vítězného uchazeče.

- Přístup na webový portál servisní podpory vítězného uchazeče v režimu 24*7 s reakční dobou danou tabulkou č. 2 viz níže.
- Telefonickou podporu nebo podporu na místě za účelem technických konzultací a řešení závad s provozní dobou 9:00 – 17:00 hod. v pracovních dnech v celkovém rozsahu 8 hod. měsíčně. V rámci kalendářního roku budou muset být nevyčerpané hodiny převedeny do následujícího období.
- Podpora dodavatele při řešení závad.

Odstranění závad bude prováděno prostřednictvím dálkového přístupu, nebude-li takové odstraněné závad možné, budou závady odstraňovány v prostorách zadavatele nebo v prostorách umístění dané komponenty. Zadavatel bude povinen umožnit vítěznému uchazeči za tím účelem dálkový přístup k dané komponentě, jakož i fyzický přístup do prostor zadavatele.

Tabulka č. 1: Kategorie závad:

Kategorie závady	Definice kategorie závady
Kritická	Komponenta zadavatele zcela selže nebo bude rozsáhle poškozena. Některé nebo všechny části softwaru podporující hlavní procesy selžou a budou zcela nefunkční nebo bude jejich funkčnost omezena tak, že bude kritickým způsobem ovlivněna činnost komponenty. Komponenta bude funkční pouze částečně.
Významná	Komponenta bude funkční pouze částečně. Komponenta bude výrazně ovlivněna z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité činnosti komponenty. Ztráta redundance komponenty.
Nízká	Komponenta bude plně operativní, pouze některé funkce budou omezeny. Závada nebude mít přímý vliv na řádný chod komponenty. Komponenta bude plně operativní.

Tabulka č. 2: Doby pro opravu závad:

Komponenta	Kategorie závady	Reakční doba (od nahlášení)	Doba odstranění závady* (od nahlášení)	Doba uvedení do původního stavu**
Skener zranitelnosti	Kritická	Následující pracovní den	3 pracovních dnů	10 pracovních dnů
	Významná	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
	Nízká	Následující pracovní den	10 pracovních dnů	10 pracovních dnů
Netflow sonda ***	Kritická	Následující pracovní den	2 pracovních dnů	10 pracovních dnů
	Významná	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
	Nízká	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
Netflow kolektor ***	Kritická	Následující pracovní den	2 pracovních dnů	10 pracovních dnů
	Významná	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
	Nízká	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
Modul detekce anomálií (NBA) ***	Kritická	Následující pracovní den	2 pracovních dnů	10 pracovních dnů

	Významná	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
	Nízká	Následující pracovní den	5 pracovních dnů	10 pracovních dnů
UTM ***	Kritická	Následující pracovní den	1 pracovní den	5 pracovních dnů
	Významná	Následující pracovní den	2 pracovních dnů	5 pracovních dnů
	Nízká	Následující pracovní den	3 pracovních dnů	10 pracovních dnů

*) V případě závady na komponentě bude vítězný uchazeč povinen zajistit náhradní prvek nebo ekvivalentní funkční komponentu, a to do doby než vadnou komponentu nahradí funkčním řešením.

**) V případě, že bude k odstranění závady potřebná implementace výrobcem vytvořeného opravného patche, bude se počítat doba uvedení do původního stavu od doby jeho uvolnění. V případě, že bude k odstranění závady potřebný HW dodávaný výrobcem, bude se počítat doba uvedení do původního stavu od doby nahlášení závady vítěznému uchazeči.

***) Zálohy konfigurací pro případnou obnovu bude zajišťovat zadavatel.

2.2 Klasifikace předmětu veřejné zakázky (CPV)

Kód předmětu veřejné zakázky dle číselníku Common Procurement Vocabulary (CPV):

32422000-7: Síťové komponenty.

3. TECHNICKÁ SPECIFIKACE KOMPONENT

V současnosti je pro potřeby bezpečnostního monitoringu nasazen IBM Security Q Radar SIEM ve formě 2100 all-in-one appliance.

V následujících bodech jsou uvedeny technické požadavky pro jednotlivé poptávané komponenty:

Skener zranitelností:

- Rozšiřující modul pro Q Radar SIEM;
- Plná integrace do rozhraní Q Radar SIEM;
- SW modul bez dodatečného HW instalovaný přímo na Q Radar 2100 appliance;
- Licence pro skenování 255 samostatných systémů.

Samostatná NetFlow sonda:

- Řešení umožňující dlouhodobé monitorování sítě na bázi protokolu NetFlow (nutná podpora NetFlow v5 a NetFlow v9) a IPFIX;
- Neviditelné na L2 a L3 vrstvě (monitorovací porty nemají IP, je zcela pasivní);
- Pasivní zapojení monitorovacích portů přes TAP nebo mirror (span) port core switche (v případě poruchy nemůže zařízení ovlivnit síť);
- Podpora pro IPv4, IPv6, VLAN;
- Monitoring 1 Gbps provozu;
- 4x1 Gbps metalické porty;
- Rack mount zařízení, 1U velikost;
- Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS;
- Možnost rozšíření o rozšiřující moduly – modul detekce anomálií;
- Součástí základní modul pro analýzu sítě: vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH).

NetFlow kolektor:

- Hardwarová appliance, disková kapacita 6TB v RAID poli;
- Jeden administrativní port 10/100/1000 Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat;
- Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS;
- Víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup;
- Podpora autentizace vůči LDAP;
- HOT SWAP disky, RAID včetně SMART detekce;
- Integrace dohledového systému pro kontrolu dostupnosti (SNMP);
- Podpora verze NetFlow protokolu – programové vybavení kolektoru musí umožnit sběr a vyhodnocení NetFlow dat ve verzi 5 a 9;
- Podpora pro sběr a analýzu sFlow a NetStream dat;
- Podpora standardů NEL a NSEL, monitorování MAC adres;
- Podpora pro příjem a analýzu informací o detekovaných aplikacích dle NBAR2 standardu;
- Podpora pro příjem a analýzu HTTP provozu - včetně položek typu URL, hostname;
- Podpora pro příjem a analýzu VoIP statistik (jitter, latence, ztrátovost);
- Možnost přeposílání přijímaných NetFlow statistik ke zpracování na další kolektory včetně možnosti filtrace na úrovni NetFlow paketů;

- Uživatelsky definovatelný dashboard (konfigurace per uživatel);
- Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH);
- Generování statistik a podrobných výpisů nad volitelnými časovými intervaly;
- Reporty v podobě průběhových i koláčových grafů;
- Online reporty včetně možnosti exportu do PDF a CSV formátu;
- Automatické zasílání reportů emailem (reporty v českém a anglickém jazyce);
- Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem);
- Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu;
- Upozornění administrátorům v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, výskyt nebezpečné anomálie, použití zakázané aplikace atd.) prostřednictví emailu, SNMP trapu a syslogu;
- Vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům (např. HTTP, FTP, SMTP, SSH provoz);
- Podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace;
- Drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami;
- Detekce aktivních zařízení na sítí - pro podporu konceptu BYOD;
- Podpora geolokace na základě IP adresy;
- Otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh.

Modul detekce anomálií na síti (NBA):

- SW modul bez nutnosti pořízení dodatečného HW;
- Sběr a zpracování statistik o síťovém provozu (NetFlow, sFlow, jFlow);
- Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů);
- Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti;
- Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti;
- Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103);
- Přehledný dashboard s okamžitou indikací problémů a top statistik;
- Integrace informací ze služeb DNS, WHOIS, geolokační služby;
- Výstup událostí protokolem Syslog pro možnost integrace do řešení Q Radar SIEM.

UTM

- Antispam, antivirus a antispyware, URL filtrace - automatické řízení web přístupů zaměstnanců;
- Integrované plnohodnotné IPS, s konfiguraci automatického vypnutí IPS ochrany v případě přetížení HW (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu;
- Ochrana VoIP provozu aplikačními proxy pro SIP a H.323;
- Filtrování internetového spojení (URL, IM, P2P, RAT, Anonymizers, …);
- IPSec VPN, průchodnost VPN 250 Mb/s;
- Licence pro konkurentní klientské připojení do VPN pomocí IPSec - min 20 kusů;
- Licence pro konkurentní klientské připojení do VPN pomocí SSL - min 20 kusů;
- Podpora VLAN;
- Cluster management (active/active nebo active/standby) s možnosti nasazení do virtuálního prostředí;
- Propustnost až 1.1 Gb/s pro aplikační kontroly;
- Non open-source;
- Antivirus a ochrana před spyware a červy na úrovni brány včetně schopnosti skenovat e-mail (SMTP), a webové (HTTP, HTTPs) přenosy v reálném čase a zjišťovat potenciální hrozby skryté uvnitř legitimního provozu;
- Vícevrstvá ochrana na úrovni brány, která je zaměřena proti hrozbám a narušením souvisejícím se spyware včetně nepřetržitě aktualizované sady anti-spyware podpisů s možností filtrování webových stránek (další proaktivní ochrana, neboť blokuje webové stránky, u kterých je známo, že distribuují spyware);
- Možnost rozšíření systému o emulace neznámých hrozeb (zero-day sandboxing) typů souborů: powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z) s možností řízení, které soubory budou zasílány na dynamickou sandbox analýzu;
- Možnost rozšíření řešení o DLP modul – počet předefinovaných datových typů (včetně lokalizovaných datových typů pro ČR), min. 500;
- Volitelná možnost zapnutí ochran pro útoky cílené na web servery (např. na přetečení buffer nebo tkz. injekce SQL, ...);
- Filtrování webových stránek;
- Site-to-site VPN propojení;
- Bezpečný flexibilní vzdálený přístup pomocí IPSec a SSL, výkonná IPSec a SSL konektivita;
- Služba vlastní certifikační autority pro vydávání PKI certifikátů pro uživatele;
- Integrovaná správa, která umožňuje z jedné konzole centrálně spravovat i více firewalů a ze které mohou administrátoři definovat a spravovat jednotlivé prvky bezpečnostní politiky: bezpečnost firewallu, překlad síťových adres (NAT), kvalitu služeb (QoS), bezpečnost VPN klientů a sítě VPN, aplikační filtrace, IPS, AV&AS;

- Centralizované automatické aktualizace;
- Monitorování v reálném čase a flexibilní vytváření reportů; centrální řízení logů s možností inkorporace zařízení třetích stran;
- Jednoduché zálohování a obnova systému (nejen částí, ale celé konfigurace);
- Možnost tvorby clusterů a vysoká dostupnost (provoz v případě nedostupnosti primárního rozhraní je směrován na sekundární rozhraní nebo ISP spoj. I během selhání se spojení udržují nepřerušená);
- Volitelný modul pro řízení (shaping) provozu VPN s přiřazováním priorit kritickým obchodním aplikacím a uživatelům pro optimalizovaný výkon.

UTM – hardware a nasazení

- Požadujeme nasazení řešení v režimu HA. Pro management je možné využít stávající VMware infrastruktury;
- Pro běh bran v režimu HA vyžadujeme:
    - Minimálně 1x procesor čtyřjádrový architektury x86, L3 cache alespoň 10MB, frekvence alespoň 2,4 GHz (s možností rozšíření na 2 procesory);
    - Paměť RAM minimálně 12 GB RAM DDR3, rozšiřitelná až na 768 GB;
    - Minimálně 2x HDD 500 GB 7200 rpm SATA, HW RAID řadič s podporou RAID 0/1/1+0;
    - Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů na Management serveru pro UTM (jeli disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky) - min. 16 TB;
    - Rozšiřitelnost až na 16 disků u Management serveru pro UTM (pouze v případě nevyužití stávající infrastruktury).
- Interní USB port kompatibilní se standardy ACPI 2.0, PCI 2.2 a USB 2.0;
- 8x UTP 1Gb Ethernet port, minimálně na dvou nezávislých NIC čipech;
- 2x 10Gb Ethernet port;
- 2x redundantní napájecí zdroj;
- Vzdálená správa: vzdálený přístup přes dedikované ethernet rozhraní, ochrana heslem, zabezpečení komunikace SSL, AES/3DES, RC4, vzdálený přístup umožňuje provést tyto operace se serverem: power on/off, reset, remote control, update BIOS, výběr bootovacího zařízení, remote control umožňuje sledovat start serveru (bios), start OS a běh OS (grafické i textové rozhraní), možnost vyvolat NMI přerušení nedostupného OS, virtuální KVM konsole, podpora virtuálních médií (CD, DVD, ISO image, USB disk, vzdálený adresář), možnost využití běžných www prohlížečů integrovaných v desktopovém OS pro správu serverů (IE, Firefox);
- Prediktivní analýza poruch na pevné disky, procesory a paměť;
- Certifikovaný Hardware pro provoz dodávaného UTM;

- Provedení do racku, rozměr max. 2RU;
- Systém musí být plně integrovatelný se systémy IBM Security Q Radar SIEM.

Návrh řešení

Uchazeč popíše způsob naplnění povinných technických parametrů jednotlivých komponent včetně značkové specifikace nabízených dodávek, a dále uvede odkaz na přiloženou část své nabídky, kde je možné ověřit naplnění požadovaného parametru. Návrh řešení uchazeč zpracuje do tabulky, jež tvoří přílohu č. 10 této zadávací dokumentace.

4. PŘEDPOKLÁDANÁ HODNOTA VEŘEJNÉ ZAKÁZKY

Předpokládaná hodnota veřejné zakázky činí 4.700.000,- Kč bez DPH. Nabídka uchazeče, která bude obsahovat nabídkovou cenu přesahující částku 4.700.000,- Kč bez DPH, nebude hodnocena a uchazeč bude zadavatelem ze zadávacího řízení vyloučen.

5. DOBA A MÍSTO PLNĚNÍ VEŘEJNĚ ZAKAZKY

5.1 Předpokládaná doba plnění

Plnění veřejné zakázky bude probíhat v následujících termínech:

- dodávka komponent a jejich implementace – tři (3) kalendářní měsíce od podpisu smlouvy na plnění veřejné zakázky;
- poskytování podpory dle bodu 2 odst. 2.1 kapitola C této zadávací dokumentace – tři (3) roky od akceptace implementace komponent.

5.2 Místo plnění veřejné zakázky

Místem plnění veřejné zakázky je sídlo zadavatele (viz také bod 1. této zadávací dokumentace).

6. KVALIFIKAČNI PŘEDPOKLADY

6.1 Kvalifikovaným pro plnění veřejné zakázky dle § 50 ZVZ je uchazeč, který:

- splní základní kvalifikační předpoklady podle bodu 6.2 této zadávací dokumentace;
- splní profesní kvalifikační předpoklady podle bodu 6.3 této zadávací dokumentace;
- předloží čestné prohlášení o své ekonomické a finanční způsobilosti splnit veřejnou zakázku podle bodu 6.4 této zadávací dokumentace;
- splní technické kvalifikační předpoklady podle bodu 6.5 této zadávací dokumentace.

6.2 Základní kvalifikační předpoklady podle § 53 odst. 1 ZVZ

Uchazeč splní základní kvalifikační předpoklady podle § 53 odst. 1 ZVZ způsobem uvedeným v § 53 odst. 3 ZVZ.

Základní kvalifikační předpoklady splňuje uchazeč, který předloží:

a) výpis z Rejstříku trestů (dle § 53 odst. 1 písm. a) a b) ZVZ);

b) potvrzení příslušného finančního úřadu (dle § 53 odst. 1 písm. f) ZVZ);

c) potvrzení příslušného orgánu či instituce (dle § 53 odst. 1 písm. h) ZVZ);

d) čestné prohlášení (dle § 53 odst. 1 písm. c) až e), f) ve vztahu ke spotřební dani, g), i) až l) ZVZ).

6.3 Profesní kvalifikační předpoklady podle § 54 písm. a) a b) ZVZ

Profesní kvalifikační předpoklady splňuje uchazeč, který předloží:

a) výpis z obchodního rejstříku nebo jiné evidence, pokud je v ní zapsán;

b) doklad o oprávnění k podnikání podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu veřejné zakázky, zejména doklad prokazující příslušné živnostenské oprávnění.

6.4 Ekonomické a finanční kvalifikační předpoklady

Uchazeč v souladu s § 50 odst. 1 písm. c) ZVZ předloží čestné prohlášení o své ekonomické a finanční způsobilosti splnit veřejnou zakázku. Čestné prohlášení bude podepsáno osobou oprávněnou jednat jménem či za uchazeče a z jeho obsahu musí vyplývat, že uchazeč splňuje požadavek zadavatele, tzn., že je ekonomicky a finančně způsobilý ke splnění veřejné zakázky. Pokud za uchazeče jedná osoba odlišná od osoby oprávněné jednat jménem či za uchazeče, musí být v nabídce předložena plná moc v originále nebo v úředně ověřené kopii.

6.5 Technické kvalifikační předpoklady podle § 56 ZVZ

6.5.1 Seznam významných zakázek

Uchazeč prokazuje splnění technických kvalifikačních předpokladů dle § 56 odst. 1 písm. a) ZVZ předložením seznamu významných zakázek formou čestného prohlášení s uvedením jejich rozsahu a doby plnění, z něhož bude vyplývat, že uchazeč v posledních třech (3) letech realizoval alespoň:

- jednu implementaci bezpečnostního monitoringu na základě IBM QRadar SIEM v hodnotě min. 1 mil. Kč bez DPH;
- jednu implementaci NetFlow řešení (Samostatná NetFlow sonda, NetFlow kolektor; Modul detekce anomálií na síti (NBA)), v hodnotě min. 1 mil. Kč bez DPH;
- jednu implementaci UTM řešení v hodnotě min. 1 mil. Kč bez DPH.

V předmětném čestném prohlášení budou uvedeny tyto údaje:

a) identifikační údaje zákazníka;

b) název významné zakázky;

c) popis významné zakázky;

d) výše plnění;

e) doba a místo realizace této významné zakázky (ve formátu MM/RRRR – MM/RRRR);

f) v případě prokazování kvalifikace postupem podle § 51 odst. 4 ZVZ identifikační údaje subdodavatele, prostřednictvím kterého uchazeč prokazuje kvalifikaci, a název a datum uzavření smlouvy podle § 51 odst. 4 písm. b) ZVZ.

Přílohou tohoto čestného prohlášení musí být:

a) osvědčení vydané veřejným zadavatelem, pokud byla významná zakázka realizována pro veřejného zadavatele, nebo

b) osvědčení vydané jinou osobou, pokud byla významná zakázka realizována ve prospěch jiné osoby než veřejného zadavatele, nebo

c) smlouva s jinou osobou a doklad o uskutečnění plnění uchazeče, není-li současně možné osvědčení podle písm. b) od této osoby získat z důvodů spočívajících na její straně.

6.5.2 Seznam členů implementačního týmu

Uchazeč rovněž prokazuje splnění technických kvalifikačních předpokladů dle § 56 odst. 1 písm. b) ZVZ předložením seznamu techniků, jež se budou podílet na plnění veřejné zakázky, bez ohledu na to, zda jde o zaměstnance uchazeče nebo osoby v jiném vztahu k uchazeči.

Zadavatel požaduje pro plnění předmětu veřejné zakázky tým zajišťující realizaci veřejné zakázky (dále jen „implementační tým“). Členové implementačního týmu, kteří musejí být dle požadavku zadavatele minimálně tři (3), musí splňovat následující požadavky (zadavatel připouští, že jedna osoba může splňovat i více požadavků na kvalifikaci uvedených techniků zároveň):

Členové implementačního týmu musí splňovat následující podmínky:

- v implementačním týmu musí být alespoň jedna (1) osoba, která má technické znalosti vlastního nabízeného řešení této veřejné zakázky (technické certifikace pro IBM QRadar SIEM) a byla zodpovědná za dodávku a implementaci alespoň tří (3) úspěšných projektů implementace QRadar SIEM v posledních třech (3) letech, kde hodnota alespoň jedné implementace přesáhla 1 mil. Kč bez DPH;
- v implementačním týmu musí být alespoň dvě (2) další osoby, které mají technické znalosti implementace QRadar SIEM (technické certifikace pro IBM QRadar SIEM) a byly součástí alespoň tří (3) úspěšných implementací QRadar SIEM v posledních třech (3) letech, kde hodnota alespoň jedné implementace přesáhla 1 mil. Kč bez DPH;
- v implementačním týmu musí být alespoň dvě (2) osoby, které mají technické znalosti implementace NetFlow sondy s NetFlow kolektorem, modulu detekce anomálií (NBA) s NetFlow kolektorem (technické certifikace nabízeného NetFlow řešení) a byly součástí implementace alespoň dvou (2) úspěšných projektů implementace NetFlow

řešení s QRadar SIEM v posledních třech (3) letech, kde hodnota alespoň jedné implementace přesáhla 1 mil. Kč bez DPH;

- v implementačním týmu musí být alespoň dvě (2) osoby mající technické znalosti implementace UTM (technická certifikace nabízené UTM) a byly součástí implementace alespoň dvou (2) úspěšných projektů implementace UTM v posledních třech (3) letech, kde hodnota alespoň jedné implementace přesáhla 1 mil. Kč bez DPH.

Seznam členů musí obsahovat:

a) celá jména všech členů implementačního týmu včetně uvedení vztahu k uchazeči (zaměstnanec, subdodavatel, jiný vztah);

b) strukturované profesní životopisy všech členů implementačního týmu;

c) požadované certifikace;

d) zahájení a ukončení realizace implementace dle podmínek výše;

e) název implementace dle podmínek výše;

f) finanční objem implementace.

Závazný jmenovitý seznam členů implementačního týmu tvoří jednu z příloh předmětné smlouvy (viz příloha č. 1 této zadávací dokumentace). Uchazeč se zavazuje plnit část předmětu veřejné zakázky týkající se projektových prací prostřednictvím členů implementačního týmu, jejichž seznam zadavateli předložil.

Uchazeč prokáže výše uvedené čestným prohlášením, přičemž při zpracování tohoto bodu může využít přílohu č. 4 této zadávací dokumentace.

6.6 Prokázání kvalifikace prostřednictvím subdodavatele

Prostřednictvím subdodavatele (subdodavatelů) může uchazeč prokázat kvalifikaci v souladu s ustanovením § 51 odst. 4 ZVZ. Uchazeč je v takovém případě povinen veřejnému zadavateli předložit:

a) doklady prokazující splnění základního kvalifikačního předpokladu podle § 53 odst. 1 písm. j) ZVZ a profesního kvalifikačního předpokladu podle § 54 písm. a) ZVZ subdodavatelem;

b) smlouvu uzavřenou se subdodavatelem, z níž vyplývá závazek subdodavatele k poskytnutí plnění určeného k plnění veřejné zakázky uchazečem či k poskytnutí věcí či práv, s nimiž bude uchazeč oprávněn disponovat v rámci plnění veřejné zakázky, a to alespoň v rozsahu, v jakém subdodavatel prokázal splnění kvalifikace.

Uchazeč není oprávněn prostřednictvím subdodavatele prokázat splnění kvalifikace dle § 54 písm. a) ZVZ.

6.7 Společná nabídka několika uchazečů

V případě podání společné nabídky několika uchazeči prokazují tito uchazeči kvalifikaci podle ustanovení § 51 odst. 5 a 6 ZVZ.

6.8 Prokázání kvalifikace zahraničním uchazečem

Zahraniční uchazeč prokazuje kvalifikaci podle ustanovení § 51 odst. 7 ZVZ.

6.9 Pravost a stáří dokladů prokazujících splnění kvalifikace

Doklady prokazující splnění kvalifikačních předpokladů předkládají uchazeči v prosté kopii. Vítězný uchazeč může být vyzván k doplnění všech listin v originále nebo ověřené kopii ve smyslu § 57 odst. 1 ZVZ. Doklady prokazující splnění základních kvalifikačních předpokladů a výpis z obchodního rejstříku nesmějí být starší 90 dnů ke dni podání nabídky.

6.10 Prokázání kvalifikace výpisem ze seznamu kvalifikovaných dodavatelů, výpisem ze seznamu certifikovaných dodavatelů nebo výpisem ze seznamu zahraničních dodavatelů

6.10.1 Uchazeči mohou k prokázání základních kvalifikačních předpokladů dle § 53 ZVZ a profesních kvalifikačních předpokladů dle § 54 ZVZ předložit výpis ze seznamu kvalifikovaných dodavatelů podle § 127 ZVZ.

6.10.2 Uchazeči mohou k prokázání kvalifikačních předpokladů předložit certifikát vydaný v rámci systému certifikovaných dodavatelů podle § 134 ZVZ. Certifikát musí obsahovat náležitosti uvedené v § 139 ZVZ a údaje v něm uvedené musí být platné nejméně k poslednímu dni lhůty pro prokázání splnění kvalifikace. Certifikát musí být platný ve smyslu § 140 odst. 1 ZVZ.

6.10.3 Zahraniční dodavatelé mohou k prokázání kvalifikačních předpokladů předložit výpis ze zahraničního seznamu kvalifikovaných dodavatelů či příslušný zahraniční certifikát podle § 143 ZVZ.

7. OBCHODNÍ A PLATEBNÍ PODMÍKY

Závazné obchodní podmínky včetně platebních podmínek, případně též objektivních podmínek, za nichž je možno překročit výši nabídkové ceny, jsou uvedeny v návrhu smlouvy, který je přílohou č. 1 této zadávací dokumentace. Tyto podmínky jsou neměnné a uchazečem mohou být doplněny pouze na vyznačených místech.

V případě nabídky podávané společně několika uchazeči je uchazeč oprávněn upravit návrh smlouvy toliko s ohledem na tuto skutečnost.

Návrh smlouvy musí být podepsán osobou oprávněnou jednat jménem či za uchazeče. Jestliže zadavatel, resp. příslušná komise zjistí, že nabídka neobsahuje návrh smlouvy nebo návrh smlouvy není podepsán vůbec či není podepsán osobou oprávněnou jednat jménem či za uchazeče, nabídku vyřadí a příslušného uchazeče zadavatel vyloučí z další účasti v zadávacím řízení.

Vybraný uchazeč je povinen po celou dobu realizace zakázky udržovat v platnosti a účinnosti pojištění odpovědnosti za škodu způsobenou třetí osobě při výkonu své podnikatelské činnosti nejméně ve výši 5.000.000,- Kč.

Tuto skutečnost prokáže uchazeč v rámci zadávacího řízení podepsáním příslušného čestného prohlášení. Čestné prohlášení o pojištění odpovědnosti za škodu je součástí čestného prohlášení, které je přílohou č. 8 této zadávací dokumentace. Vybraný uchazeč je povinen před podpisem smlouvy a následně kdykoliv na požádání zadavatele prokázat splnění této podmínky předložením kopie platné pojistné smlouvy či certifikátu.

8. POŽADAVKY NA VARIANTY NABÍDEK

Zadavatel nepřipouští variantní řešení dle § 70 ZVZ.

9. POŽADAVKY NA ZPUSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

Uchazeč do nabídky uvede na zvláštním listě (vzor tvoří přílohu č. 9 této zadávací dokumentace) nabídkovou cenu v členění dle tabulek uvedených v předmětném vzoru v české měně (CZK). Uchazeč doplní hodnoty pouze DO NEPODBARVENÝCH POLÍ. Celková nabídková cena pro účely hodnocení se bude nacházet v tučně ohraničeném poli v tabulce č. 4 předmětného vzoru – přílohy č. 9 této zadávací dokumentace (celková nabídková cena je složena z ceny za dodávku všech komponent, maximální výše za provedení projektových prací a ceny za tři roky podpory k jednotlivým komponentám). Celkovou nabídkovou cenu poté uchazeč doplní v požadovaném členění do krycího listu (rovněž výši DPH a cenu vč. DPH) a nabídkové ceny rovněž rozepíše do závazného vzoru předmětné smlouvy.

Celková nabídková cena nesmí překročit částku uvedenou v bodě 4. této zadávací dokumentace.

10. POKYNY PRO ZPRACOVÁNÍ A ČLENĚNÍ NABÍDKY, DALŠÍ POŽADAVKY ZADAVATELE NA PŘEDLOŽENÍ DOKUMENTŮ

10.1 Uchazeč může podat pouze jednu nabídku. Uchazeč, který podal nabídku v zadávacím řízení, nesmí být současně subdodavatelem, jehož prostřednictvím jiný uchazeč v tomtéž zadávacím řízení prokazuje kvalifikaci. Pokud uchazeč podá více nabídek samostatně nebo společně s dalšími uchazeči, nebo je subdodavatelem, jehož prostřednictvím jiný uchazeč v tomtéž zadávacím řízení prokazuje kvalifikaci, zadavatel všechny nabídky podané takovým uchazečem vyřadí. Uchazeče, jehož nabídka byla vyřazena, zadavatel bezodkladně vyloučí z další účasti v zadávacím řízení. Vyloučení uchazeče včetně důvodu zadavatel bezodkladně písemně oznámí uchazeči v souladu se ZVZ.

10.2 Nabídka:

- bude předložena ve dvou (2) vyhotoveních (originál + kopie) v listinné podobě, v českém jazyce;
- nesmí obsahovat přepisy a opravy, které by mohly zadavatele uvést v omyl;

- musí obsahovat návrh smlouvy vč. doplněných příloh podepsaný oprávněnou osobou jednat jménem či za uchazeče i v elektronické podobě na CD/DVD nosiči (příloha č. 1 této zadávací dokumentace);
- bude obsahovat vyplněný krycí list nabídky (příloha č. 2 této zadávací dokumentace);
- bude obsahovat doklady, jimiž uchazeč prokazuje splnění kvalifikace;
- bude obsahovat doklady v souladu s § 68 odst. 3 ZVZ:
    - seznam statutárních orgánů nebo členů statutárních orgánů, kteří v posledních 3 letech od konce lhůty pro podání nabídek byli v pracovněprávním, funkčním či obdobném poměru u zadavatele;
    - má-li uchazeč formu akciové společnosti, seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě pro podání nabídek;
    - prohlášení uchazeče o tom, že neuzavřel a neuzavře zakázanou dohodu podle zákona č. 143/2001 Sb., o ochraně hospodářské soutěže, ve znění pozdějších předpisů, v souvislosti se zadávanou veřejnou zakázkou;
- bude obsahovat vyplněné tabulky o zpracování nabídkové ceny (viz příloha č. 9 této zadávací dokumentace);
- bude obsahovat návrh řešení (vyplněné tabulky) dle bodu 3. této zadávací dokumentace (viz příloha č. 10 této zadávací dokumentace);
- bude obsahovat ostatní dokumenty požadované zadavatelem (doklady, čestná prohlášení, plnou moc apod.).

10.3 Zadavatel doporučuje uchazečům, aby:

- své nabídky zabezpečil proti manipulaci;
- všechny listy nabídky byly navzájem pevně spojeny či sešity, tak aby byly zabezpečeny před jejich vyjmutím z nabídky;
- všechny stránky nabídky byly očíslovány vzestupnou kontinuální řadou.

10.4 Zadavatel doporučuje uchazečům, aby strukturovali nabídku v následujícím členění:

- obsah nabídky;
- vyplněný krycí list nabídky;
- doklady, jimiž uchazeč prokazuje splnění kvalifikace;
- vlastní nabídka uchazeče a související doklady;
- návrh řešení;
- návrh smlouvy;
- zpracování nabídkové ceny;
- ostatní doklady a prohlášení požadované zadavatelem.

10.5 V případě zjištění neetických praktik uchazeče spočívajících v nabízení, poskytnutí, přijímání nebo zprostředkování nějakých hodnot nebo výhod s cílem ovlivnit chování nebo jednání kohokoliv přímo nebo nepřímo v zadávacím řízení či rozporu čestného prohlášení uchazeče a skutečností ověřených zadavatelem na základě spolehlivých informací, případně i na základě požádání uchazeče o písemné vysvětlení nebo po přizvání uchazeče pro ústní vysvětlení, vyloučí zadavatel takového uchazeče bezodkladně ze zadávacího řízení.

Při předkládání nabídky musí uchazeč předložit čestné prohlášení o neexistenci střetu zájmů a v něm prohlásit, že není v zadávacím řízení ovlivněn přímo ani nepřímo střetem zájmů ve vztahu k zadavateli, ani k subjektům podílejícím se na přípravě tohoto zadávacího řízení, jakož i že nemá žádné zvláštní spojení s těmito osobami (např. majetkové, personální).

11. HODNOCENÍ NABÍDEK

Základním hodnotícím kritériem je nejnižší nabídková cena bez DPH (zpracovaná dle bodu 9 této zadávací dokumentace) dle § 78 odst. 1 písm. b) ZVZ. Nabídky budou hodnoceny dle § 79 odst. 4 zákona.

Pro číselně vyjádřitelné dílčí hodnotící kritérium (nabídková cena celkem bez DPH), pro které má nejvhodnější nabídka minimální hodnotu, získá hodnocená nabídka bodovou hodnotu, která vznikne násobkem 100 a poměru hodnoty nejvhodnější nabídky k hodnocené nabídce.

Tento popis způsobu hodnocení lze matematicky vyjádřit pomocí následujícího vzorce:

body = (nejnižší nabídková cena/nabídková cena) x 100.

Při hodnocení nabídek hodnotící komise seřadí jednotlivé nabídky vzestupně tak, že na první místo umístí nabídku s nejnižší nabídkovou cenou a na poslední místo nabídku s nejvyšší nabídkovou cenou.

12. JISTOTA

Zadavatel nepožaduje poskytnutí jistoty dle § 67 ZVZ.

13. DODATEČNÉ INFORMACE K ZADÁVACÍM PODMÍNKÁM

Uchazeči mohou písemně požadovat po zadavateli dodatečné informace k zadávacím podmínkám. Písemná žádost o dodatečné informace musí být doručena zadavateli v souladu s § 49 odst. 1 ZVZ nejpozději 6 pracovních dnů před uplynutím lhůty pro podání nabídek. Požadované informace k zadávacím podmínkám pak zadavatel poskytne ve lhůtě a způsobem dle § 49 odst. 2 a 3 ZVZ.

Zadavatel může poskytnout uchazečům dodatečné informace i bez předchozí žádosti v souladu s ustanovením § 49 odst. 4 ZVZ.

14. PROHLÍDKA MÍSTA PLNĚNÍ

Prohlídka místa plnění se vzhledem k charakteru předmětu veřejné zakázky neuskuteční.

15. LHŮTA A MÍSTO PRO PODÁNÍ NABÍDEK, OTEVÍRAŃÍ OBÁLEK S NABÍDKAMI

15.1 Lhůta a místo pro podání nabídek

Nabídky se podávají písemně a v řádně uzavřené obálce opatřené na uzavřeních označením obchodní firmy nebo razítkem či podpisem statutárního orgánu uchazeče nebo osoby oprávněné jednat jménem či za uchazeče.

Obálka musí být označena nápisem **„Nabídka – Neotevírat – Samostatné oddělení veřejných zakázek 240“** a názvem veřejné zakázky, tj. **„SIEM – rozvoj zabezpečení rezortní sítě“** a musí dále obsahovat adresu uchazeče, na niž je možné zaslat vyrozumění podle § 71 odst. 5 ZVZ.

Lhůta pro podání nabídek končí dne 15. 04. 2016 v 10:00 hod.

Nabídky je možné podat osobně na podatelně v sídle zadavatele v PO a ST v době od 07:30 do 17:00 hod, v ÚT a ČT v době od 7:30 do 16:30 hod a v PÁ v době od 7:30 do 15:00 hod (v poslední den lhůty pouze do 10:00 hod), či zaslat na adresu sídla zadavatele (viz bod 1. této zadávací dokumentace).

Nabídku, která bude podána po uplynutí lhůty pro podání nabídek, komise neotevře. Zadavatel si takovou nabídku ponechá a uchazeče vyrozumí o tom, že nabídka byla podána po uplynutí lhůty pro podání nabídek.

15.2 Otevírání obálek s nabídkami

Otevírání obálek s nabídkami proběhne dne 15. 04. 2016 od 10:30 hod v sídle zadavatele.

Otevírání obálek s nabídkami se může účastnit max. 1 zástupce uchazeče, jehož nabídka byla podána ve lhůtě pro podání nabídek. Při otevírání obálek s nabídkami se tito uchazeči prokáží oprávněním k účasti na otevírání obálek s nabídkami (např. plnou mocí vystavenou osobou oprávněnou jménem či za uchazeče jednat).

V době od konce lhůty pro podání nabídek do začátku otevírání obálek provede zadavatel kontrolu oprávnění k účasti jednotlivých účastníků, zajistí jejich podpis do prezenční listiny, uvede účastníky do jednací místnosti, kde se bude otevírání obálek s nabídkami konat, a provede případně další nezbytné úkony směřující k otevírání obálek s nabídkami.

16. ZADÁVACI LHŮTA

Uchazeč je svou nabídkou vázán po dobu 90 dní ode dne konce lhůty pro podání nabídek.

17. POSKYTOVÁNÍ ZADÁVACÍ DOKUMENTACE

Zadávací dokumentace k této veřejné zakázce včetně všech příloh a případných dodatečných informací bude po celou dobu lhůty pro podání nabídek uveřejněna neomezeným a přímým dálkovým přístupem na profilu zadavatele: https://ezak.mzp.cz.

18. PŘÍLOHY ZADAVACÍ DOKUMENTACE

1. Návrh smlouvy včetně technické specifikace;
2. Krycí list nabídky (vzor);
3. Čestné prohlášení o splnění základních kvalifikačních předpokladů (vzor);
4. Čestné prohlášení k prokázání splnění technických kvalifikačních předpokladů (vzor);
5. Čestné prohlášení o ekonomické a finanční způsobilosti (vzor);
6. Čestné prohlášení dle § 68 odst. 3 ZVZ (vzor);
7. Čestné prohlášení o subdodavatelích (vzor);
8. Čestné prohlášení o neexistenci střetu zájmů a souhlasu se zadávacími podmínkami (vzor);
9. Zpracování nabídkové ceny;
10. Návrh řešení.

V Praze dne 22. 02. 2016

Ing. Jana Vodičková
ředitelka odboru informatiky
Česká republika – Ministerstvo životního prostředí