Příloha č. 1 výzvy k podání nabídky

**TECHNICKÁ SPECIFIKACE A POŽADAVKY**

k veřejné zakázce malého rozsahu s názvem
**„Systém pro správu a analýzu logů“**Registrační číslo projektu: CZ.06.01.01/00/22\_010/0002965

1. **Účastník zpracuje technickou část nabídky** podle této osnovy, která bude nedílnou součástí nabídky a připojí ji jako přílohu č. 1 návrhu smlouvy.
2. **Účastník zpracuje** **v technické části nabídky detailní popis nabízeného systému pro správu a analýzu logů**, zejména:

- specifikaci technických údajů (výrobce, typ licence…) včetně technického popisu;

**-** rozsah a způsob poskytování technické podpory (detailní popis, který bude v souladu s čl. XI. návrhu smlouvy);

**-** předpokládaný rozsah součinnosti objednatele (detailní popis, který bude v souladu s čl. VII. návrhu smlouvy);

**-** předpokládaný termín dodávky.

**Součástí technické části nabídky zpracované účastníkem bude vyplněná verifikační tabulka uvedená níže, která bude podkladem pro provedení akceptačních testů (viz čl. V návrhu smlouvy).**

**Zadavatel požaduje:**

Dodat clusterovou hardwarovou appliance sloužící jako centrální úložiště logů pro sběr a analýzu bezpečnostních událostí z kritických systémů, serverů, aplikací a koncových stanic (včetně záruky na hardware a softwarové subscription na období 60 měsíců); součástí dodávky je instalace a implementace (tj. konfigurace a uvedení do provozu) do prostředí IS ÚMČ Praha 12 a vytvoření nezbytné dokumentace a zaškolení určených osob.

Zajistit technickou a záruční podporu v délce trvání 60 měsíců.

Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze systému, funkce zařazené na tzv. roadmapu nebudou akceptovány. Pokud jakákoli níže uvedená funkcionalita vyžaduje licenci, tak tato licence musí být součástí nabídky i nabídkové ceny.

**Nabízený systém pro správu a analýzu logů musí splňovat parametry dle níže uvedené verifikační tabulky:**

Nabízený systém pro správu a analýzu logů musí splňovat parametry dle níže uvedené verifikační tabulky. **Účastník je povinen vyplněnou tabulku přiložit do své nabídky.**

Účastník vyplní vždy sloupec „Nabízené zařízení splňuje minimální požadavky: „ANO/NE“. V případě, uvedení slova „ANO“ specifikuje blíže naplnění parametru (pokud je bližší specifikace možná).

V případě uvedení slova „NE“ může být nabídka vyloučena ze zadávacího řízení z důvodu nesplnění povinných požadavků pro účast v zadávacím řízení.

|  |  |  |  |
| --- | --- | --- | --- |
| **Bod** | **Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno) a požadované funkce** | **Splněno ANO/NE** | **Stručný popis plnění** |
|  |  |  |  |
|  | **1.      Softwarové požadavky** |   |   |
|  |  |  |  |
| 1 | Systém se chová jako jeden celek s jedním komplexním rozhraním administrátora i operátora. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 2 | Systém dokáže zpracovávat událostí z definovaných zdrojů logů nezávisle na výrobci aplikací, operačních systémů nebo síťových komponent pokud splňují alespoň syslog formát (viz bod 3). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 3 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně protokolu UDP/TCP 514 (SYSLOG). Systém musí umožnovat příjem logů i na uživatelsky definovaných UDP a TCP portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 4 | Systém umožňuje tvorbu parseru pro zařízení která nejsou zarhnuta v defaultně dodaných parserech. A to uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 5 | Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje ji a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. Tj. každá přijatá zpráva má dvě časové značky a obě je možné uživatelsky zobrazit. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 6 | Všechny zprávy přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 7 | Ve správcovské konzoli (viz bod 18) nesmí být možnost mazání nebo modifikování již uložených logů bez ohledu na přiřazenou roli.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 8 | Systém umožňuje snadné vyhledávání v událostech (ad hoc) bez nutnosti dodatečného vytváření skriptů či nutnosti používat regex dotazy.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 9 | Systém provádí komplexní vizualizaci logů, událostí a dat (grafy událostí). Vizualizace musí být dynamická, tj. volba na jednom grafu se propisuje na příslušné grafy v pohledu a ty se následně upraví dle požadované volby automaticky. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 10 | Systém má možnost snadno zobrazit grafickou podobu TOP událostí nad všemi daty za určitý definovaný časový úsek. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 11 | Systém provádí automatické doplňování GeoIP informací k událostem a poskytuje jejich grafické znázornění na mapě bez nutnosti instalovat či napojovat služby třetích stran či externích aplikací. Je možné využít službu třetí strany, pokud dodavatel tuto službu zajistí a implementuje do systému.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 12 | Systém umožňuje doplňování reverzních DNS záznamů k IP adresám z logů. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 13 | V případě přetížení jakékoliv části systému nesmí dojít ke ztrátě přijatých dat. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším vytížení paměti musí být administrátor systému automaticky informován.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 14 | Správcovské prostředí musí obsahovat reportovací nástroj s přednastavenými nejběžnějšími dashboardy a zároveň musí mít možnost definování a uložení uživatelem vytvořených přehledů nebo dashboardů. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 15 | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 16 | Systém nabízí kapacitní i výkonovou škálovatelnost bez nutnosti reinstalace nebo výrazné rekonfigurace systému. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 17 | Systém musí obsahovat REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožnovat autorizovaný přístup ke strukturované databázi logů. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 18 | Systém obsahuje jednotnou centrální webovou konzoly pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není možné, aby dodaný systém měl více konzolí pro různé části systému. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 19 | Systém musí umožňovat snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému. Je případně možné využít již definované role např. administrátora a operátora. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 20 | Systém musí parsování a normalizaci přijatých událostí provádět bez nutnosti instalovat externí aplikace nebo agenty, a to přímo ve svém rozhraní. Přípustnou výjimkou je monitoring systémů Windows, kde WMI protokol neumožňuje monitorovat logy.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 21 | Systém musí podporovat ověřování uživatele z nejméně dvou externích Active Directory / LDAP serverů. V případě výpadku LDAP systému musí být možnost přihlášení lokálním účtem. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 22 | Systém musí být dimenzován na zpracování minimálně 50 milionů eventů denně a nebo denní přírůstek dat alespoň 90 GB. Zadavatel v současnosti sbírá data přibližně z 60 zařízení, přičemž výhledově se může počet zdrojových systémů rozšířit až na cca 400 zařízení (včetně serverů a koncových stanic). V případě potřeby může zadavatel poskytnout doplňující informace k předpokládané infrastruktuře nebo charakteru logovaných dat. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 23 | Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace vendora zařízení podle MAC adresy. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 24 | Možnost on-line testování uživatelsky definovaných parserů - při jejich tvorbě je možné otestovat vlastní zprávy, při změně je okamžitě zobrazen výsledek rozparsovaných dat a případná chybová hlášení. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 25 | V centrální konzoli (viz bod 18) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 26 | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 27 | Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert a ten odeslat. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 28 | Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 29 | Systém musí obsahovat předpřipravené sety/vzory alertů dodaných výrobcem. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 30 | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP a Syslogu přes TCP protokol. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 31 | V alertech je možné využít značky (příklad: informuj uživatele jen v případě, že se událost stala na serveru, který běží v lokalitě XY). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 32 | Události z Microsoft prostředí mohou být vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 33 | Systém podporuje zajištění sběru nemodifikovaných událostí a detailní zpracování auditních informací. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 34 | Pokud budou události vyčítány pomocí agenta, pak musí mít agent buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 35 | Pokud budou události vyčítány pomocí agenta, pak musí být komunikace agenta a centrálního systému šifrovaná. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 36 | Pokud budou události vyčítány pomocí agenta, pak musí agent podporovat sběr dat nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 18) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 37 | Pokud budou události vyčítány pomocí agenta, pak musí agent automaticky doplňovat ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 38 | Řešení ukládá logy do zaplnění kapacity přiděleného místa a následně odmazává nejstarší záznamy.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 39 | Případný počet instalací (licencí) Windows agenta není limitován počtem licencí. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 40 | Systém musí umožňovat retenci minimálně 365 dní při průměrném příjmu 3 tisíce EPS. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 41 | Systém splňuje požadavky dané zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění, včetně připravované novely tohoto zákona implementující evropskou směrnici NIS2 do českého právního řádu. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 42 | Systém musí obsahovat mechanismus, který zajistí nezaměnitelnost záznamů logů (např. hashovaní). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 43 | Systém musí být schopný běžet offline, tj. sběr dat nesmí pro svou funkčnost vyžadovat konektivitu do internetu. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 44 | Systém se chová jako jeden celek s jedním komplexním rozhraním administrátora i operátora. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 45 | Systém dokáže zpracovávat událostí z definovaných zdrojů logů nezávisle na výrobci aplikací, operačních systémů nebo síťových komponent pokud splňují alespoň syslog formát (viz bod 3). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
|  |  |  |  |
|  | **2.      Hardwarové požadavky** |  |  |
|  |  |  |   |
| 46 | Systém podporuje provoz ve 2 oddělených appliance formou clusteru a tento zajištuje sběr dat i při výpadku celé jedné appliance.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 47 | Řešení musí umožnit snadné zálohování a plnohodnotnou obnovu celé konfigurace bez potřeby složitého zásahu správce nebo ručních zásahů do souborů zálohy. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 48 | Zařízení musí mít možnost instalace do standardizovaného 19" RACKu a dodávka musí být vč. montážního materiálu a kolejnic. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 49 | Zařízení se musí vejít do maximální hloubky 105 cm a současně do svislé rozteče vertikálních kolejnic nepřesahující 74 cm. Celková výšková velikost zařízení v jedné lokalitě nesmí přesáhnout 6U. V případě potřeby je možné si vyžádat bližší specifikaci tohoto omezení před podáním nabídky. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 50 | Dodavatel dodá napájecí kabely s koncovkou C13 pro zapojení do PDU | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 51 | Zařízení má standartní airflow (zepředu dozadu). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 52 | Propoj do infrastruktury realizován pomocí metalické sítě s RJ45 konektory na rychlosti minimálně 1Gbit. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 53 | Možnost nastavit LACP (IEEE 802.3ad). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 54 | Systém má oddělený monitoring vč. oddělených portů pro monitoring HW (iLo, iDRAC apod). | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 55 | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, 2x PSU apod.) a je nezávislá na dalších systémech. Výjimku tvoří případné externí uložiště, které musí ve stejné konfiguraci jako server (2x PSU, min 2x 1Gbit komunikační port a dedikovaný port pro monitoring HW) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 56 | Úložiště pro integrovanou databázi podporovanou HW akcelerovaným RAID řadičem. Řadič musí disponovat zálohovací baterii nebo být vybaven flash pamětí. Velikost uložiště musí být navržena tak, aby splnila požadovanou retenci z bodu 43.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 57 | Server obsahuje minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Pokud je dodáno externí diskové pole, musí splňovat stejné parametry. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 58 | Větráky v systému musí být vyměnitelné za provozu a redundantní. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 59 | 2x napájecí zdroje s redundancí napájení 1+1. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 60 | Systém pro vzdálenou správu serveru vč. KVM (iLo, iDRAC, IPMI apod.). Dodávka včetně potřebné licence, pokud je třeba. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 61 | HW - požadovaná servisní podpora min. 60 měsíců na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 62 | SW – podpora výrobce na aktualizaci systému (subscription – nárok na aktuální verze) a parserů min. na 60 měsíců. Podpora musí obsahovat aktualizaci SW, opravy a telefonickou a e-mailovou podporu.  | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 63 | Platba za dodávku bude realizována formou jediné platby. Technická podpora následně platbou ročně. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 64 | Součástí dodávky je předání dokumentace k systému. Tj. zapojení HW prvků, popisy portů, umístění, nastavení jednotlivých appliance, přístupy, vč. nastavení délek logování, emergency účtů apod. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 65 | Dodavatel provede zaškolení obsluhy, a zajistí, aby školitel mluvil českým jazykem a to na úrovni rodilého mluvčího. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 66 | Dodavatel prohlašuje, že neobchoduje se sankcionovaným zbožím, které se nachází v Rusku nebo Bělorusku či z Ruska nebo Běloruska pochází a nenabízí takové zboží v rámci plnění veřejných zakázek. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |