**Příloha č. 2 zadávací dokumentace**

**Technická specifikace a požadavky zadavatele**

**Stávající stav:**

**Zadavatel** provozuje systém pro sběr, analýzu a korelace logů a jejich dlouhodobou důvěryhodnou archivaci (forenzní archív) technické zařízení **Logmanager** .

Stávající technické zařízení **Logmanager** je **umístěno v** datovém centru zadavatele v lokalitě Pardubická nemocnice a tvoří 2 nodový vysoce dostupný cluster.

Zařízení Logmanager rovněž používají i zdravotnická zařízení Pardubického kraje, kde je do budoucna možná vzájemná spolupráce nad sběrem a vyhodnocováním logů v centrálním systému Logmanager umístěným v datovém centru nemocnice Pardubice, určeným pro centralizovaný sběr, ukládání a analýzu logů z vybraných zdravotnických zařízení Pardubického kraje.

**Předmět plnění veřejné zakázky**

Předmětem plnění je dodávka **hardwarové technologie** pro centrální sběr, analýzu a archivaci logů (dále jen **log management**) dle podrobné specifikace a požadavků uvedených dále v této příloze***.*** Cílem této dodávky je realizovat nový 2-nodový cluster pro log management a realizovat vysoce výkonnou a dostupnou architekturu log managementu v organizaci. Celé dodávané řešení musí být funkční jako celek a jedno místo sběru logů.

**Logem** se rozumí časově označený záznam události nebo aktivity, která se odehrála v informačním systému, aplikaci, technickém zařízení nebo počítačové síti.

Vysoce dostupné řešení sběru logů s architekturou 2-nodového clusteru využívá pro zajištění vysoké dostupnosti systém FortiGate zadavatele, který monitoruje dostupnost obou zařízené a řídí provoz na tomto clusteru. Zadavatel požaduje zachovat a dále využívat tuto funkcionalitu i v rámci nového řešení, pokud tuto skutečnost neřeší dodávané řešení vlastními prostředky nebo funkcionalitou.

Stávající technické zařízení LogManager zadavatele využívá komponenty Logmanager Forwarder, které slouží pro sběr logů z lokalit s nestabilním připojením kde se objevují občasné výpadky sítě. Zadavatel požaduje v rámci dodávaného řešení zachovat tuto funkcionalitu pro překlenutí těchto výpadků.

Požadujeme dodávku a implementaci celého řešení a zprovoznění všech požadovaných funkcí v rámci dodávky. Nepřipouští se žádné doplňování požadovaných funkcí v budoucnu nebo nějaký budoucí dovývoj požadované funkcionality.

**\*\*\*\*\*\*\*\*\***

**Dodávané řešení systému pro log management musí splňovat uživatelské a technické požadavky na dílo, jak je uvedeno v tabulce dále Tabulka 1: Požadovaná funkcionalita a vlastnosti.**

Technologie pro centrální sběr, analýzu a archivaci logů (dále jen **log management**) je též označována pojmy jako Systém, Řešení, Dodávané řešení apod. - všechny tyto označení jsou ekvivalentní a označují stejný předmět.

Uvedené požadavky jsou, pokud není uvedeno jinak, minimální.

**Všechny požadované funkce musí být dodány v rámci dodávky** a být přístupné bez dalších nákladů, a to včetně požadavků (funkcí) formulovaných jako „Možnost, schopnost, …“.

**Tabulka 1: Požadovaná funkcionalita a vlastnosti**

|  |  |  |
| --- | --- | --- |
| **Požadovaná funkcionalita a vlastnosti** | | **Splnění**  Ano/Ne |
| **A** | **Obecné požadavky** |  |
| 1 | **Dodávané řešení musí umožnit:** |  |
| 2 | centrální sběr, analýzu a ukládání logů ze všech lokalit organizace |  |
| 3 | vytvoření důvěryhodného archivu pro forenzní analýzu logů |  |
| 4 | realizaci vysoce dostupného (HA) clusteru s využitím stávající technologie |  |
| 5 | zpracování událostí z logů různých typů aplikací, síťových zařízení a operačních systémů od různých výrobců, v souladu se seznamem v tabulce ***Tabulka 2: Vyžadovaná podporovaná zařízení a aplikace*** |  |
| 6 | Uživatelské konfigurační rozhraní musí být v jazyce českém. |  |
| 7 | Uživatelská dokumentace musí být k dispozici v českém i anglickém jazyce |  |
|  |  |  |
| **B** | **Základní požadavky** |  |
| 1 | Dodávané řešení musí být realizováno jako hardwarová appliance s jednotným webovým rozhraním pro veškeré administrátorské i operátorské úlohy. |  |
| 2 | Pro veškeré administrátorské i uživatelské činnosti musí být k dispozici s jednotné webové rozhraní. |  |
| 3 | Nastavování a konfigurace musí být proveditelná vlastními prostředky systému log managementu, nepřipouští se nutnost užití programování a znalost specifického programovacího jazyka |  |
| 4 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím protokolu Syslog (RFC5424) a minimálně těchto dalších protokolů: RELP, RAW, CEF, LEEF, JSON (RFC8259) |  |
| 5 | Systém podporuje sběr logů minimálně z těchto databázových systémů MSSQL, PostgreSQL, Oracle a MySQL |  |
| 6 | Systém provádí jednotnou normalizaci logů (převod do jednotného formátu) |  |
| 7 | Systém uchovává originální logy v jejich původním formátu. |  |
| 8 | Systém poskytuje kompletní řešení pro parsování a normalizaci událostí bez nutnosti externích aplikací. |  |
| 9 | Systém musí umožnit vytvářet uživatelské parsery pro dosud nepodporovaná zařízení, bez nutnosti změn konfiguračních souborů pouze s užitím uživatelského rozhraní. |  |
| 10 | Systém umožňuje automatické přidávání meta informací k událostem a to i v rámci uživatelských definovaných parserů. |  |
| 11 | Systém musí umožnit přetypování parsovaných a ukládaných hodnot na základní datové typy (jako URL, IP adresa, MAC adresa aj.) |  |
| 12 | Systém musí vytvářet vlastní důvěryhodné časové značky při přijetí logu. |  |
|  |  |  |
| **C** | **Požadavky na technické a výkonové parametry** |  |
| 1 | Systém je dodáván jako soubor hardwarových appliancí, včetně lyžin pro snadnou instalaci do racku. |  |
| 2 | Každá hardwarová appliance obsahuje minimálně 2 x SFP+, 4× 1Gbit LAN porty a 1× dedikovaný 1Gbit port pro správu hardwaru včetně SFP modulů 10Gbit typu MultiMode. |  |
| 3 | Každá hardwarová appliance je vybavena redundantními ventilátory s možností výměny za provozu. |  |
| 4 | Každá hardwarová appliance obsahuje 2 napájecí zdroje s možností výměny za provozu. |  |
| 5 | Systém obsahuje integrované řešení pro vzdálenou správu, včetně licence pro provoz po dobu trvání podpory hardware výrobcem (ekvivalentní technologiím jako HP iLO, Dell iDRAC apod.) |  |
| 6 | Systém disponuje minimálně 160TB diskové kapacity clusterového řešení pro ukládání logů a dalších dat. |  |
| 7 | Systém dodává aktualizace ve formě jednotného balíčku, který lze nainstalovat přímo prostřednictvím centrální webové správcovské konzole, bez potřeby přístupu k operačnímu systému serveru nebo použití příkazového řádku. |  |
| 8 | Systém trvale dosahuje průměrného příjmu alespoň 9 000 událostí za sekundu při zprávách o průměrné délce minimálně 700 bajtů. Informace vychází z aktuálního stavu příjmu událostí a predikovaného růstu. |  |
| 9 | Systém je schopen zvládnout špičkový příjem alespoň 18 000 událostí za sekundu po dobu minimálně 5 minut. |  |
| 10 | Systém umožňuje příjem událostí z neomezeného počtu zařízení bez licenčních omezení. Počet zpracovaných událostí není licenčně omezen na základě objemu dat v GB za den, ani počtu zdrojových zařízení. V případě, že je systém licenčně omezen, musí být schopen přijímat a zpracovávat data minimálně z 1 500 zdrojových zařízení o objemu alespoň 500 GB logů denně. |  |
| 11 | Dodávaný systém podporuje nasazení ve vysoce dostupném clusterovém řešení a má nativní podporu pro nastavení HA clusteru. |  |
| 12 | Systém musí poskytovat informace o stavu clusteru a jeho konfiguraci. |  |
| 13 | Systém musí poskytovat informace o stavu synchronizace databází mezi jednotlivými nody. |  |
| 14 | Systém umožňuje export dat ve formátu vhodném pro strojové zpracování, bez omezení množství či obsahu exportovaných záznamů. Při exportu lze volitelně definovat konkrétní pole, která mají být do výstupu zahrnuta. |  |
| 15 | Systém podporuje zálohování a obnovení konfigurace pro celý systém. |  |
|  |  |  |
| **D** | **Sběr logů** |  |
| 1 | Řešení musí umožňovat centrální správu konfigurace sběru logů, včetně selektivního zapínání nebo vypínání konkrétních zdrojů logů, změny nastavení bez nutnosti ručního zásahu na jednotlivých zařízeních a okamžitého nebo plánovaného rozeslání nové konfigurace. |  |
| 2 | Systém musí umožnit definovat ke každému zpracovanému logu jedinečný a dohledatelný identifikátor, který zajišťuje jeho jednoznačnou identifikaci. |  |
| 3 | Systém umožňuje nativní sběr logů z prostředí Office 365/Microsoft 365 nezávisle na typu licence a bez potřeby instalace dalších externích komponent. |  |
| 4 | Systém umožňuje sběr logů z prostředí Microsoft a poskytuje možnost centrální konfigurace logovacích politik, bez nutnosti využívat řízení pomocí GPO. |  |
| 5 | Systém umožňuje sběr logů i ze zařízení mimo doménu. |  |
| 6 | Systém umožňuje filtrování událostí na straně Windows před samotným odesláním logu, čímž snižuje objem přenášených a zpracovávaných dat. |  |
| 7 | Přenos logovaných dat z koncových zařízení do centrálního systému musí probíhat šifrovaným komunikačním kanálem, splňujícím současné bezpečnostní standardy (např. TLS 1.2 nebo vyšší). |  |
| 8 | Požadujeme zachovat funkcionalitu pro sběr logů z lokalit s nestabilním připojením kde se můžou objevovat občasné výpadky sítě. |  |
| 9 | Řešení automaticky navazuje spojení s centrálním datovým úložištěm, zabezpečuje přenos dat šifrováním a v případě výpadku spojení automaticky obnovuje připojení. |  |
| 10 | Řešení musí umožňovat sběr systémových událostí (např. operační systém, bezpečnostní protokoly) z koncových zařízení a serverů. |  |
| 11 | Musí být zajištěn sběr logovacích dat i z lokálních souborových zdrojů na těchto zařízeních (např. logovací soubory aplikací, služeb nebo systémových komponent). |  |
| 12 | Musí být umožněno hromadné nasazení sběrné komponenty, pokud je pro sběr logů použita, (např. prostřednictvím běžných nástrojů pro správu IT – Active Directory, Group Policy, skripty, balíčky pro vzdálené nasazení apod.) na stovky až tisíce zařízení. |  |
| 13 | Systém musí disponovat funkcionalitou pro automatickou detekci výpadku sběru logů z konkrétního zařízení, včetně možnosti generování upozornění nebo výstrah k případnému výpadku sběru logů. |  |
| 14 | Řešení musí zachovat sběr logů z kritických informačních systémů organizace jako je např. klinický informační systém, (KIS), stravovací systém (SIS) a další. |  |
| 15 | Systém musí umožňovat sběr logů z aplikací a systémových komponent, které vyžadují vyšší oprávnění (např. root, SYSTEM účet, služby běžící jako LocalSystem). |  |
|  |  |  |
| **E** | **Notifikace** |  |
| 1 | Systém umožňuje uživatelům nastavovat podmínky pro upozornění, která jsou automaticky vyvolána při jejich splnění v přijatých datech. |  |
| 2 | Systém umožňuje uživatelskou úpravu textu e-mailu generovaného vybranou událostí (alertem) a podporuje vložení proměnných, které jsou automaticky vyplněny na základě rozparsované události. |  |
| 3 | Systém umožňuje nastavování alertů a korelací prostřednictvím grafického rozhraní. |  |
| 4 | Systém umožňuje odeslání vybraných událostí (alertů) na externí systém. |  |
| 5 | Systém umožňuje nejen využívat značky/tagy ve vybraných událostech (alertech), ale také je přiřazovat na základě definovaných podmínek. |  |
|  |  |  |
| **F** | **Výstupy** |  |
| 1 | Systém poskytuje dynamickou vizualizaci sbíraných událostí (logů) ve formě grafů. |  |
| 2 | Systém umožňuje okamžité prohledávání historických dat bez nutnosti importu nebo dekomprese a bez nutnosti manuální konfigurace nebo zásahů uživatele. |  |
| 3 | Systém umožňuje vytváření uživatelských pohledů na uložené události a export těchto dat |  |
| 4 | Systém musí umožnit definici pravidel pro filtrování událostí podle důležitosti a nastavení předávaní těchto událostí dle těchto pravidel. |  |
| 5 | Systém musí umožnit filtraci nerelevantních událostí. |  |
| 6 | Nastavení definice pravidel filtrování musí být realizována prostředky grafického uživatelského rozhraní. |  |
|  |  |  |
| **G** | **Řízení přístupových práv** |  |
| 1 | Systém musí mít implementováno řízení uživatelských rolí a přístupových práv. |  |
| 2 | Systém přístupových práv musí umožnit řídit přístup k událostem podle typu filtrů |  |
| 3 | Systém musí podporovat napojení na systém řízení přístupů AD/LDAP. |  |
| 4 | Systém musí podporovat rovněž přihlášení pomocí lokálních účtů. |  |
|  |  |  |
| **H** | **Forenzní archív** |  |
| 1 | Systém musí garantovat neměnnost uložených logů po celou dobu stanovené retenční doby. Jakékoli mazání či úpravy logů, včetně zásahů ze strany administrátorů musí být znemožněny. |  |
| 2 | Nová řešení musí zachovat všechna uložená data logů (historická data) uložená v archivu do doby změny současného stavu na nové řešení. |  |
| 3 | Dodávané řešení musí umožnit migraci dat ze stávajících systémů sběru logů buď formou synchronizace databází nebo jinou formou dle určení dodavatele tak, aby v době převzetí projektu do užití byly data zmigrována a totožná na všech úložištích systému pro sběr logů. |  |
| 4 | Systém musí v provedení HA clusteru synchronizovat databáze nodů v reálném čase. |  |
|  |  |  |
| **I** | **Možnost integrace na systémy analýzy bezpečnostních událostí minimálně:** |  |
| 1 | Systémy SIEM pomocí standardních protokolů (např. WAZUH SIEM, FortiSIEM, MS Sentinel aj.) |  |
|  |  |  |
| **J** | Požadovaná dokumentace |  |
| 1 | Uživatelský manuál |  |
| 2 | Dokumentace výrobce k technickým parametrům (datasheety) |  |
| 3 | Implementační plán projektu |  |

|  |  |  |
| --- | --- | --- |
| **Z** | **Záruční podmínky** | **Splnění**  Ano/Ne |
| 1 | Je požadována 5-letá servisní podpora výrobce hardwarových appliancí na tyto appliance i na dodávaní řešení jako celek. |  |
| 2 | Tato 5-letá servisní podpora výrobce musí zahrnovat: |  |
|  | opravu technických závad přímo na místě instalace a garantovanou odezvou následující pracovní den po nahlášení závady |  |
|  | softwarové aktualizace, opravy softwarových chyb |  |
|  | možnost telefonické i e-mailové podpory přímo s výrobcem/dodavatelem |  |
|  | možnost podpory s diagnostikou přes vzdálený přístup |  |
|  |  |  |

**Ověření funkčních vlastností**

Dodavatel předvede na žádost zadavatele funkční vzorek nabízeného řešení pro sběr, analýzu a archivaci logů formou osobní prezentace. Pod pojmem **funkční vzorek** rozumí zadavatel funkční instalaci nabízeného řešení, prostřednictvím kterého bude dodavatel schopen dokumentovat (prezentovat formou ukázky živého systému) funkčnost nabízeného řešení. Funkční vzorek zadavatel specifikuje takto:

**2 ks zařízení v identické konfiguraci s nabízeným systémem v režimu vysoké dostupnosti**

**Pro předvedení platí tyto pravidla:**

1. V případě konání praktické ukázky funkčnosti systému bude termín prezentace sdělen danému dodavateli řešení nejpozději 7 kalendářních dnů přede dnem konání.
2. Místem konání prezentace je místnost ředitele úseku ICT, budova č. 10, nemocnice Pardubice
3. Doba trvání prezentace bude max. 120 minut. Do doby prezentace se nepočítá doba instalace technologie do datového centra, nastavení a vzorového sběru dat.
4. Za každého z účastníků zadávacího řízení se mohou prezentace zúčastnit nejvýše čtyři osoby. Účastníci se prokáží dokladem prokazujícím oprávnění jednat jménem dodavatele, případně plnou mocí vystavenou osobou oprávněnou jednat jménem dodavatele.
5. Během prezentace nebude přípustné pokládat členům hodnotící komise jakékoliv dotazy.
6. Z prezentace bude vyhotoven protokol o konání prezentace, který bude na závěr jednání podepsán oběma stranami.
7. Zadavatel poskytne dodavateli řešení prostor v racku v datovém centru na budově č. 10 v nemocnici Pardubice, elektrické napájení, síťovou konektivitu a určí 5 vybraných systémů pro sběr logů.
8. Zadavatel požaduje realizovat sběr logů z určených systémů po dobu 7 dnů od zprovoznění řešení, než bude provedena vlastní prezentace.

Tabulka níže specifikuje vybrané požadavky na prokázání požadovaných vlastností řešení:

|  |  |  |
| --- | --- | --- |
|  | **Podklady pro ověření požadovaných vlastností a specifikací** | **Splnění**  Ano/Ne |
| 1 | Dodavatel řešení provede základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření vzorových uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému. |  |
| 2 | Dodavatel řešení připojí pět vybraných zdrojových systémů logů, které odesílají logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a předvede způsob, jak se provádí (nebo je realizováno):  nastavení klasifikace zdrojů  nastavení značek (tagů) pro vybrané zdrojové systémy  filtrování událostí. |  |
| 3 | Dodavatel řešení ukáže způsob vytváření reportů generovaných systémem i uživatelsky. |  |
| 4 | Dodavatel řešení ukáže způsob provádění exportu logů a vybraných údajů z logů. |  |
| 5 | Dodavatel řešení provede konfiguraci tří vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému. |  |
| 6 | Dodavatel řešení prokáže nezměnitelnost logů uložených v nabízeném systému ověřením shody uložených logů s originálními logy v systému Windows na vybraném vzorku logů. |  |
| 7 | Konfigurace sběru logů z databázových systémů v prostředí zadavatele realizovat v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran. |  |
| 8 | Dodavatel předvede obnovení funkčnosti nabízeného systému po simulovaném úplném selhání ze záloh v následujících krocích:  provedení zálohy konfigurace na externí úložiště dat (např. na NAS systém)  vytažení libovolného disku za běhu systému  nastavení systému do továrního nastavení  obnovení konfigurace z vytvořených záloh  kontrola úplnosti obnovené konfigurace ze záloh. |  |
| 9 | Kontrola výkonu systému v běžné zátěži – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. |  |
| 10 | K bodu 9 bude dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace. |  |
| 11 | Dodavatel předvede funkčnost HA clusteru simulací výpadku jednoho nodu. |  |
|  |  |  |

**Tabulka 2: Vyžadovaná podporovaná zařízení a aplikace**

|  |  |
| --- | --- |
| **Podporovaná zařízení** | **Splněno** (Ano/Ne) |
| Apache httpd |  |
| Apache Tomcat |  |
| Antivir Eset |  |
| Brocade FC switches |  |
| ArcSight CEF format all sources |  |
| Cisco ASA |  |
| Cisco IOS |  |
| Cisco IronPort |  |
| Cisco Nexus |  |
| Cisco SMB |  |
| Cisco WLC |  |
| Dell Force10 |  |
| Dell iDrac (Server OoB management) |  |
| Dell PowerConnect |  |
| Dell SonicWALL |  |
| FlowMon |  |
| FortiAuthenticator |  |
| FortiDDoS |  |
| Fortigate |  |
| FortiGate-Lite (performance optimized) |  |
| FortiMail |  |
| FortiManager |  |
| FreeRADIUS |  |
| Qradar LEEF format all sources |  |
| HPE Aruba Instant AP (WLAN) |  |
| HPE Aruba Mobility Controller (WLAN) |  |
| HPE iLo 4 (Server OoB management) |  |
| HPE IMC |  |
| HPE routers |  |
| HPE switches Procurve OS |  |
| HPE switches Comware OS |  |
| HPE Comware WLAN |  |
| Huawei USG |  |
| ISC BIND |  |
| ISC DHCP |  |
| ISC DHCPD |  |
| JSON format all sources |  |
| Juniper SRX |  |
| Juniper SRX-Lite (performance optimized) |  |
| Linux Cron |  |
| Linux Freeradius |  |
| Linux Iptables |  |
| Linux Postfix |  |
| LOGmanager |  |
| Mikrotik |  |
| Microsoft Exchange log |  |
| Microsoft SharePoint |  |
| Microsoft SQL |  |
| Microsoft Windows DHCP log |  |
| Microsoft Windows DNS debug log |  |
| Microsoft Windows Firewall (optimized for performance) |  |
| Microsoft Windows IIS |  |
| MySQL |  |
| Nginx |  |
| OpenSSH server |  |
| Oracle DB |  |
| Palo Alto Networks NGFW |  |
| PostgreSQL |  |
| Ruckuss wireless |  |
| SAP |  |
| Sophos |  |
| RFC5425 format all sources |  |
| Symantec Endpoint Protection Manager |  |
| Symantec Messaging Gateway (brightmail) |  |
| Synology NAS DSM |  |
| UBNT Rocket |  |
| UBNT UniFI |  |
| VMware |  |
| Windows - any logs from Event Viewer |  |
| Windows - any text log from file |  |
| Fons Enterprise |  |
| System Kredit Anete |  |
| OverLaps for Windows Laps - text log from file |  |