**Příloha č. 4 – Technická specifikace**

**Technická specifikace**

|  |  |  |  |
| --- | --- | --- | --- |
| **Číslo** | **Popis** | **Splňuje ANO/NE** | **Poznámka** |
|  | **Obecné požadavky na systém (minimální, nepodkročitelné)** |  |  | |
| 1 | Systém pracuje jako hardware appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací vyjma agenta pro sběr Windows logů. | Ano |  |
| 2 | Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. | Ano |  |
| 3 | Systém umožňuje dopsání parseru pro nová zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem 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. | Ano |  |
| 4 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožnovat přijímat logy i na uživatelsky definovaných UDP a TPC 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. | Ano |  |
| 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. | Ano |  |
| 6 | Všechny pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování. | Ano |  |
| 7 | Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159. | Ano |  |
| 8 | Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. | Ano |  |
| 9 | Systém provádí konsolidaci logů na centrálním místě. | Ano |  |
| 10 | Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. | Ano |  |
| 11 | Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. | Ano |  |
| 12 | Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě. | Ano |  |
| 13 | Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám. | Ano |  |
| 14 | V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. | Ano |  |
| 15 | Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení. | Ano |  |
| 16 | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data pro budoucí zpracování. | Ano |  |
| 17 | Systém podporuje průběžné aktualizace systému výrobcem. | Ano |  |
| 18 | Konfigurační a Systémové rozhraní a dokumentace musí být identické v anglickém i v českém jazyce. | Ano |  |
| 19 | Systém nabízí kapacitní i výkonovou škálovatelnost. | Ano |  |
| 20 | Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB. | Ano |  |
| 21 | Požadujeme, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště. | Ano |  |
| 22 | Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému. | Ano |  |
| 23 | Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožnoval autorizovaný přístup ke strukturované databázi logů. | Ano |  |
| 24 | Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému. | Ano |  |
| 25 | Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. | Ano |  |
| 26 | Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes WMI protokol neumožňuje monitorovat textové logy. | Ano |  |
| 27 | Systém musí podporovat ověřování uživatele systému na externím AD serveru. V případě výpadku AD systému musí podporovat ověření z lokální databáze. Šifrování uživatelských údajů pomocí BCrypt. | Ano |  |
|  | **Minimální HW parametry požadovaného systému (minimální, nepodkročitelné)** |  |  |
| 28 | Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. | Ano |  |
| 29 | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech. | Ano |  |
| 30 | 2 procesory (min. 10 jader každý), podpora HyperThreadingu. | Ano |  |
| 31 | Min. 64GB DDR4 | Ano |  |
| 32 | Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. | Ano |  |
| 33 | Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček. | Ano |  |
| 34 | Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. | Ano |  |
| 35 | Větráky v systému musí být vyměnitelné za provozu a redundantní. | Ano |  |
| 36 | 2x napájecí zdroje s redundancí napájení 1+1. | Ano |  |
| 37 | Virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. | Ano |  |
| 38 | Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). | Ano |  |
|  | **Výkonnostní a SW parametry systému (minimální, nepodkročitelné)** |  |  |
| 39 | Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli - viz bod 29, není nutné editovat žádné konfigurační soubory včetně IP adresace systému). | Ano |  |
| 40 | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli (viz bod 29). | Ano |  |
| 41 | Systém musí podporovat downgrade, pro případ problémů s novou verzí systému po upgrade. | Ano |  |
| 42 | Průměrný trvalý příjem min. 5 tis. událostí/s s možností navýšení na minimálně 10 tis. událostí/s prostřednictvím licence nebo rozšíření hardware. | Ano |  |
| 43 | Špičkový příjem 10 tis. událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. | Ano |  |
| 44 | Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200 GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat. | Ano |  |
| 45 | Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz bod 29). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |  |
| 46 | Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení. | Ano |  |
| 47 | V centrální správcovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. | Ano |  |
| 48 | V centrální správcovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.). | Ano |  |
| 49 | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | Ano |  |
| 50 | Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active/active. | Ano |  |
| 51 | Vícenodový systém se chová jako 1 celek. | Ano |  |
| 52 | V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru. | Ano |  |
| 53 | Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru. | Ano |  |
| 54 | V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody. | Ano |  |
|  | **Alerty (minimální, nepodkročitelné)** |  |  |
| 55 | Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert. | Ano |  |
| 56 | Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události. | Ano |  |
| 57 | Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |  |
| 58 | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. | Ano |  |
| 59 | V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě XYZ). | Ano |  |
|  | **Sběr událostí z Microsoft prostředí (minimální, nepodkročitelné)** |  |  |
| 60 | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů. | Ano |  |
| 61 | Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací. | Ano |  |
| 62 | Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole z bodu 29. | Ano |  |
| 63 | Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |  |
| 64 | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzoly systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy. | Ano |  |
| 65 | Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.). | Ano |  |
| 66 | Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů. | Ano |  |
| 67 | Komunikace Windows agenta a centrálního systému musí být šifrovaná. | Ano |  |
| 68 | Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. | Ano |  |
| 69 | Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. | Ano |  |
| 70 | Počet instalací Windows agenta nesmí být licenčně omezen. | Ano |  |
|  | **Podpora a záruka (minimální, nepodkročitelné)** |  |  |
| 71 | Hardware - Požadovaná min. 5-ti letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | Ano |  |
| 72 | Software - Podpora výrobce na aktualizaci systému a parserů na **1 rok.** Podpora musí obsahovat aktualizaci SW, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem. | Ano |  |

**Implementace**

Zhotovitel provede tyto práce:

* Nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele.
* Konfigurace systémů a zařízení zadavatele tak, aby posílaly logy do testovaného systému:
  + - Switch: HP1820 – 9x, HP1920 – 8x, HP2910 – 2x, HP5500 – 2x, HP5900AF – 2x, Aruba 2530 24G PoE+ Switch J9773A – 10x, Aruba 2530 24G Switch J9776A – 5x, Aruba 2530 48G PoE+ Switch J9772A – 15x, Aruba 2530 48G Switch J9775A – 8x
    - Firewall: Fortigate 200B – 2x, Fortigate 500E – 2x.
* Instalace Windows agenta na systémy požadované zadavatelem a jeho konfigurace – viz Technická specifikace, odstavec „Sběr událostí z Microsoft prostředí“ – 60 MS severů.
* Konfigurace systému pro komunikaci s nainstalovanými Windows agenty.
* Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným zaměstnancům zadavatele – jeden vzorový dashboard.
* Vytvoření alertu specifikovaného zadavatelem – viz Technická specifikace, odstavec SW parametry a odstavec Alerty (příklad: pošli alert jen v případě, že se událost stala na kritickém Windows serveru, který běží v lokalitě XYZ).

**Support (SW):**

1 rok  (8 hodin, 5 dní v týdnu – pondělí až pátek), a to v rozmezí: od …… hod. *(mezi 7.00 hod. a 8.00 hod. - časový údaj doplní účastník)* do …… hod. *(mezi 15.00 hod. a 16.00 hod. - časový údaj doplní účastník. Čas musí odpovídat celkovým 8 hodinám)*

Předmět a rozsah supportu zahrnuje zejména:

hardwarovou jednotku, výměnu hardwaru, firmware a všeobecné aktualizace.

Účastník doloží technické parametry technickým listem výrobce systému nebo jiným dokumentem prokazujícím splnění minimálních technických požadavků.