# 7 Centrální logovací nástroj

## Definice předmětu zakázky:

Součástí projektu bude návrh, dodávka a implementace systému pro sběr a analýzu logů s pokročilými nástroji pro „Alerting“. Systém bude sloužit jako jednotné úložiště logů z připojených stávajících i nově dodávaných systémů Zadavatele a musí umožňovat následnou základní analýzu bezpečnostních událostí z připojených systémů a aplikací.

Systém může být dodán ve formě fyzického zařízení, nebo jako virtuální řešení. V případě nabídnutí virtuálního řešení musí na tuto skutečnost dodavatel jednoznačně upozornit a veškerý HW (ESX hosty jako nový cluster a pole v obou lokalitách, SAN/Ethernet transceivery, atd.) a případné související licence musí být součástí nabídky datového centra jako samostatně označený celek a řešení nesmí jakkoli omezovat kapacitu, ani výkonnost poptávaného datového centra. Výkon a kapacity hw pro virtuální řešení musí být odpovídající výkonu a kapacitě fyzické appliance. Systém v případě virtualizovaného řešení musí být provozován na platformě VMware ESXi.

Systém musí umožnovat bezztrátový sběr a příjem událostí ze zdrojů v odloučených lokalitách.

Systém musí umožňovat jednotné ukládání a uchovávání provozních dat a logů po dobu vyžadovanou ZKB, resp. prováděcí vyhláškou VKB v aktuálním znění. Nezbytnou nutností v rámci legislativních požadavků je podpora uchovávání originálních logů pro účely případného bezpečnostního auditu, a tudíž i vyloučení možnosti modifikace logů ze strany administrátorů nebo uživatelů. Dále je vyžadována funkcionalita automatického reportování událostí/incidentů a aktivit uživatelů/administrátorů v uživatelsky definovaném rozsahu.

Systém musí disponovat funkcionalitou sledování chování uživatelů a systémů s možností upozorňování na překročení pravidel definovaných uživateli/administrátory v rámci konfigurace, nebo nastavení systému, a to na základě limitů nebo korelací událostí. Součástí funkcionality systému je i pravidelný automatický reporting.

Dodaný systém musí disponovat jednotným grafickým rozhraním, které umožňuje kompletní konfiguraci a následnou správu systému uživateli/administrátory. Toto rozhraní musí být dostupné minimálně v české a anglické jazykové mutaci. Rozhraní musí umožnit procházení aktuálních i uložených logů vhodným grafickým nástrojem s předdefinovanými pravidly pro rychlé filtrování a vyhledávání.

Systém bude sloužit k záznamu a zpracování událostí z předdefinovaných zdrojů logů nezávisle na výrobci aplikací, operačních systémů a hardware a musí disponovat sadou předdefinovaných parserů pro běžně užívaná technologická zařízení. Musí podporovat minimálně Zadavatelem používaná zařízení definovaná přílohou (viz 7\_Priloha\_-\_Seznam\_vyzadovanych\_podporovanych\_systemu).

Systém umožňuje prostřednictvím jednotného grafického rozhraní uživatelskou/administrátorskou konfiguraci vlastních parserů pomocí vizuálního programovacího jazyka bez nutnosti zásahu výrobce nebo dodavatele a bez nutnosti dodatečného programování nebo znalostí SQL syntaxe. Součástí dodávky a implementace bude dokumentace v českém jazyce, která poskytne jednoznačný návod tvorby parseru, včetně vzorových příkladů a zaškolení odpovědných pracovníků Zadavatele.

## Technická specifikace předmětu zakázky:

|  |  |  |
| --- | --- | --- |
| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| **Obecné požadavky na systém Centrálního logovacího nástroje** | | |
| Systém dodávaný jako appliance, nebo virtuální řešení (viz. textová část předmětu dodávky) se sjednoceným grafickým rozhraním pro kompletní administrátorskou i operátorskou obsluhu. | ANO |  |
| Dodávka nevyžaduje instalaci dalších systémů a aplikací s výjimkou podpory sběru z detašovaných lokalit a agentů pro sběr logů z OS MS Windows. | ANO |  |
| Systém slouží k záznamu a zpracování událostí z předdefinovaných zdrojů logů nezávisle na výrobci aplikací, operačních systémů a síťového hardware a musí podporovat minimálně zařízení definovaná přílohou (viz 7\_Priloha\_-\_Seznam\_vyzadovanych\_podporovanych\_systemu). | ANO |  |
| Systém musí umožnit uživatelskou definici parseru pro výše neuvedená zařízení bez nutnosti spolupráce s výrobcem nebo dodavatelem/subdodavatelem nabízeného systému. | ANO |  |
| Parsery a alerty a to jak předdefinované, tak i uživatelské musí umožňovat využití matematických operací. | ANO |  |
| Parsery a alerty a to jak předdefinované, tak i uživatelské musí podporovat dekódování URL. | ANO |  |
| Systém musí umožnit přijímání a zpracovává logů, události/incidentů a další strojově generovaných dat prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). | ANO |  |
| Systém musí umožnovat příjem logů i na uživatelsky definovaných UDP a TPC portech. Standardizaci přijatých logů systém do jednotného formátu a logy jsou rozdělovány do příslušných polí dle jejich typu. | ANO |  |
| Systém musí umožnovat uchovávání i originální verze zpráv. | ANO |  |
| Systém musí umožnit zachování původní informace ze zdroje logu o časové značce události, ale nedůvěřuje ji a vytváří vlastní časové razítko ke každému logu, kterému systém důvěřuje a kterým se řídí. | ANO |  |
| Všechna pole a položky přijaté systémem musí být automaticky indexovány tak, aby bylo možné ihned provádět vyhledávání. | ANO |  |
| Systém musí umožnovat sběr událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159. | ANO |  |
| Systém musí zajistit nemodifikovatelnost uložených logů. Pro každý log musí být vytvořen unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. | ANO |  |
| Systém musí umožňovat na základě konfigurací definovaného pravidla nebo parseru přijatou zprávu zahodit. | ANO |  |
| Systém musí umožňovat konsolidaci logů na centrálním místě. | ANO |  |
| Systém musí umožnit snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo znalostí SQL syntaxe. | ANO |  |
| Grafické rozhraní systému musí umožňovat komplexní dynamickou vizualizaci logů, událostí/incidentů a strojových dat. (grafy událostí). | ANO |  |
| Systém musí umožňovat snadnou definici grafického znázornění TOP událostí nad všemi daty za určitá časová období. | ANO |  |
| Systém musí být schopen automaticky doplňovat GeoIP informace k událostem/incidentům a jejich následné grafické znázornění na mapě bez nutnosti využívat 3rd party služeb nebo externích aplikací. | ANO |  |
| Systém umožňuje automaticky doplňovat reverzní DNS záznamy k IP adresám. | ANO |  |
| Systém zajišťuje bezztrátovost logů v případě přetížení. Veškeré nezpracované logy, události /incidenty přijaté v rámci stavu přetížení jsou ukládány do vyrovnávací paměti (minimální velikost vyrovnávací paměti je 50 GB). | ANO |  |
| Při výrazném zaplnění vyrovnávací paměti systém automaticky informuje administrátora/y. | ANO |  |
| Systém umožňuje uživateli/administrátorovi jednoduché konsolidované vyhledávání napříč všemi typy dat a připojených zařízení. | ANO |  |
| Systém umožňuje uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. | ANO |  |
| Systém zahrnuje reportovací nástroj s výrobcem přednastavenými základními reporty a umožňuje definici vlastních pohledů. A to bez nutnosti dodatečného programování nebo znalostí SQL syntaxe. | ANO |  |
| Grafické rozhraní systému obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií připojených zdrojových zařízení s přihlédnutím na logické členění. | ANO |  |
| Systém umožňuje automatizovanou aktualizaci reportů a pohledů výrobcem. | ANO |  |
| Konfigurační a Systémové rozhraní systému je identické v anglickém i v českém jazyce. | ANO |  |
| Kapacita úložného prostoru (Disková kapacita appliance/pole, případně dedikovaná kapacita v rámci DC) pro systémem uložená data (logy, události /incidenty přijaté systémem) je 100TB. (v závorce uveďte dodávanou kapacitu) | ANO |  |
| V rámci vysoké dostupnosti systém umožňuje vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Systémem použitá metoda zabezpečení dat proti selhání (RAID) neovlivňuje požadovanou kapacitu úložiště. | ANO |  |
| Systém umožňuje monitoring stavu - "alertování" při překročení definovaných prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog. | ANO |  |
| Systém obsahuje REST-API pro integraci s externím monitorovacím systémem (PRTG, Zabbix, Nagios, MRTG a další) a umožňuje autorizovaný přístup ke strukturované databázi logů. | ANO |  |
| Systém disponuje jednotnou centrální webovou konzolí pro kompletní správu systému a přístup k logům, alertům a reportům. Není přípustné, aby dodávaný systém měl více konzolí pro jednotlivé funkční celky systému. | ANO |  |
| Systém umožňuje snadné vytváření uživatelských rolí včetně definice přístupových práv k uloženým datům (logy, události /incidenty přijaté systémem) a řídícím komponentám systému. | ANO |  |
| Systém umožňuje parsování a normalizaci přijatých událostí bez nutnosti instalovat další externí aplikace nebo systémy, a to přímo prostřednictvím svého rozhraní. Povolenou (očekávanou) výjimku tvoří systém pro monitorování OS MS Windows. | ANO |  |
| Systém umožňuje navázat ověřování uživatele systému na externí LDAP server. Pro případ výpadku externího LDAP serveru podporuje systém ověření proti lokální databázi. | ANO |  |
| **Minimální požadavky na HW řešení požadovaného systému bude-li řešeno formou appliance** | | |
| HW appliance obsahující všechny potřebné systémové komponenty (Procesory, RAM, diskový prostor), nezávislá na dalších systémech. max. 2U | ANO |  |
| Minimálně 2 procesory (každý min. 12 jader) s podporou HyperThreadingu. | ANO |  |
| RAM minimálně 128 GB DDR-4. V závorce uveďte hodnotu RAM. | ANO |  |
| Disková kapacita minimálně 100TB s akcelerovaným SAS RAID řadičem s read-write cache min. 4 GB pro systémovou databázi. V závorce uveďte nabízenou diskovou kapacitu. | ANO |  |
| Disková kapacita je z výkonnostních důvodů tvořena minimálně 12 ks stejných disků určených pro použití v datacentrových úložištích, min. 7200 otáček/s. V závorce uveďte počet disků. | ANO |  |
| Řadič diskového pole obsahuje zálohovací baterii nebo je osazen flash pamětí. | ANO |  |
| Síťová konektivita min 4x 1Gbit LAN + 1x dedikovaný 1Gbit port pro management HW. | ANO |  |
| Appliance používá pro chlazení minimálně 2 za provozu vyměnitelné větráky. | ANO |  |
| Napájení appliance je zajištěno minimálně dvěma na sobě nezávislými napájecími zdroji vyměnitelnými za chodu schopnými při výpadku jednoho zajistit bez omezení funkčnost systému. | ANO |  |
| Systém disponuje virtuální KVM pro zajištění vzdáleného ovládání a rozšířený systém pro vzdálenou správu serveru včetně případné licence. | ANO |  |
| **Požadavky na výkonost a SW parametry systému** | | |
| Všechny části systémů lze nastavit z centrální administrátorské konzole grafického rozhraní systému bez nutnosti manuální editace konfiguračních souborů. | ANO |  |
| Systém umožňuje stálý příjem min. 10 tis událostí /s při průměrné velikosti události 600 Byte. | ANO |  |
| Systém umožňuje nejméně po dobu 10 minut špičkový příjem minimálně 20 tis událostí/incidentů / s, v případě vyššího počtu událostí/incidentů jsou tyto ukládány systémem do bufferu k pozdějšímu zpracování. | ANO |  |
| Systém nemá licenčně omezený počet zařízení zasílajících události, ani jinak licenčně omezený počet událostí za den. | ANO |  |
| Integrovaná systémová databáze má čistou velikost nejméně 100 TB s možností aktivace komprese ukládaných dat. | ANO |  |
| Systém umožňuje prostřednictvím jednotného grafického rozhraní uživatelskou/administrátorskou konfiguraci vlastních parserů pomocí vizuálního programovacího jazyka (viz bod 33) bez nutnosti dodatečného programování nebo znalostí SQL syntaxe. | ANO |  |
| Grafické rozhraní administrátorské konzole (viz bod 33) umožňuje přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení atd. | ANO |  |
| Grafické rozhraní administrátorské konzole (viz bod 33) umožňuje při definici vlastního parseru přidávat značky pro typy událostí (login, logout apod.). | ANO |  |
| Systémem přidávané značky jsou ukládány pro každou přijatou událost/incident, a na jejich základě je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | ANO |  |
| Konfigurace uživatelských parserů umožňuje automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy. | ANO |  |
| Systém umožňuje on-line ladění uživatelsky definovaných parserů - v rámci přípravy je možno vložit do systému vlastní testovací zprávy, jejichž výsledná podoba a případná chybová hlášení je okamžitě zobrazena. | ANO |  |
| Systém podporuje integraci externích informací. | ANO |  |
| Pro případné budoucí využití zvýšené dostupnosti podporuje systém zrcadlení a cluster – min. 2 nody v režimu active / active. | ANO |  |
| Dvou a více nodový cluster se chová jako 1 celek. | ANO |  |
| Je-li využito clusteru tvořeného dvěma, nebo více nody jsou automaticky prohledávána všechna data na všech zařízeních v clusteru. | ANO |  |
| Jestliže je využit dvou a více nodový system, podporuje řešení přijímání událostí/incidentů na jednu virtuální adresu a cluster automaticky zajišťuje synchronizaci událostí/incidentů mezi nody. | ANO |  |
| Systém obsahuje mezipamět diskového subsystému v provedení SSD nebo NVRAM s kapacitou minimálně 3TB. | ANO |  |
| Systém podporuje zálohování a obnovení konfigurace v jednom kroku s využitím jednoho souboru pro celý systém. | ANO |  |
| **Alerty a systémová hlášení** | | |
| Systém je schopen generovat alerty na základě splnění uživatelem / administrátorem zadaných podmínek. | ANO |  |
| Textace alertů jsou uživatelsky/administrátorsy definované a umožňují vkládání proměnných na základě přijatých rozparsovaných události/incidentů. | ANO |  |
| Systém disponuje sety výrobce předpřipravených alertů, které jsou dále uživatelsky/administrátorsky modifikovatelné. | ANO |  |
| Systém podporuje konfiguraci alertů pomocí vizuálního programovacího jazyka, který není prezentován textově, ale pomocí piktogramů zastupujících aplikační logiku v grafickém jednotného rozhraní systému. | ANO |  |
| Systém umožňuje pro jednotlivé Alerty nadefinovat výstupní pravidlo/pravidla, která zajistí odeslání originální události, která alert vyvolala prostřednictvím SMTP nebo Syslogu přes TCP protokol do externí ho systému. | ANO |  |
| Systém podporuje alespoň základní funkci pro korelace událostí/incidentů a upozornění s hraničními limity. | ANO |  |
| **Sběr událostí z prostředí OS Microsoft Windows** | | |
| Systém umožňuje vyčítání událostí z prostředí OS Microsoft pomocí agenta instalovaného přímo v koncových systémech. Agent musí zároveň podporovat monitoring interních windows logů i monitoring textových souborových logů. | ANO |  |
| Agent systému umožňuje sběr nemodifikovaných událostí/incidentů pro detailní zpracování auditních informací. | ANO |  |
| Agent systému umožňuje uživatelské/administrátorské nastavení filtrace odesílaných událostí pomocí grafického rozhraní jednotné administrátorské konzole z bodu 33. | ANO |  |
| Agent systému pro vyčítání událostí/incidentů z OS MS Windows umožňuje správu a automatickou aktualizaci z centrální konzole systému (viz bod 33). | ANO |  |
| Agent systému automaticky překládá zástupné kódy ve zprávách na textové informace. | ANO |  |
| Agent systému pro vyčítání událostí/incidentů z OS MS Windows má buffer pro případ ztráty spojení mezi centrálním úložištěm logů a koncovým systémem, ze kterého jsou události/incidenty vyčítány. | ANO |  |
| Všechna data odesílaná klientským Agentem systému do centrálního systému jsou šifrovaná. | ANO |  |
| Agent systému pro vyčítání událostí/incidentů umožňuje spolu se systémovými logy (Aplikace, Zabezpečení, Instalace, Systém) i rozšířený sběr logů ve složce Protokoly aplikací a služeb. Toto nastavení je prováděno prostřednictvím centrální administrátorské konzole systému. | ANO |  |
| Agent systému umožňuje ke všem odesílaným událostem/incidentům automatické doplnění jejich textového popisu zobrazeného v "Prohlížeči událostí (Event Viewer) koncového systému. | ANO |  |
| Počet instalací Windows agenta koncových systémů je minimálně 1500 licencí aktivních licencí, nebo není licenčně omezen. | ANO |  |
| **Podpora pro sběr událostí z odloučených lokalit** | | |
| Systém zahrnuje řešení pro sběr události v odloučených lokalitách a umožňuje jejich bezztrátové šifrované odeslání prostřednictvím datové linky do centrálního systému. | ANO |  |
| Nabízený systém podporuje centralizovanou správu pro sběr událostí přímo z jednotného grafického rozhraní centrálního systému. | ANO |  |
| Dojde-li k výpadku spojení mezi odloučenou lokalitou a centrální lokalitou naváže/obnoví systém spojení automaticky včetně zabezpečení šifrováním, a to bez nutnosti zásahu uživatele/administrátora. | ANO |  |
| Systém umožňuje komunikovat pomocí definovaného IP protokolu, aby bylo možno využít prioritizace služeb v rámci přenosu dat mezi centrálou a odloučenou lokalitou. | ANO |  |
| Systém disponuje kapacitou vyrovnávací paměti pro minimálně 100 GB událostí/incidentů, které mohou vzniknout v odloučené lokalitě v průběhu výpadku spojení mezi lokalitou a centrálním systémem. | ANO |  |
| Systém sběru dat z odloučených lokalit má minimální výkon 5 tisíc událostí /s. a to i při trvalé zátěži. | ANO |  |
| Systém podporuje pro UDP i TCP zdroje a pro aktivní sběr událostí/incidentů z OS MS Windows pomocí agentů. | ANO |  |
| Systém sběru dat z odloučených lokalit je k dispozici jako fyzický systém nebo jako virtuální systém na platformě VMware ESXi či Hyper-V. | ANO |  |
| Systém sběru dat z odloučených lokalit umožňuje komunikaci na centrální lokalitu i přes vícenásobný překlad adres (NAT). | ANO |  |
| **SW podpora a záruka na hardware** | | |
| V rámci dodávky je požadovaná min. 5letá servisní podpora na hardware appliance s opravou v místě instalace a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | ANO |  |
| V rámci dodávky je požadovaná min. 5letá servisní podpora výrobce na SW včetně aktualizací systému a parserů. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně včetně její implementace, bezodkladnou reakci na opravy bezpečnostních chyb, telefonickou a e-mailovou podporu. | ANO |  |
| **Dokumentace** | | |
| Dokumentace musí obsahovat přehledný návod na tvorbu zákaznických parserů v českém jazyce a systém musí obsahovat možnost testování a ladění vytvářených zákaznických parserů a to bez vlivu na ostatní provozní funkce. | ANO |  |
| Dokumentace je významově i obsahově identická v anglickém i v českém jazyce. Omezená dokumentace v českém jazyce není přípustná. | ANO |  |
| Dodavatel předloží zadavateli potvrzení vystavené autorizovanou osobou o shodě nabízeného systému s požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení nesmí být nahrazeno/zaměněno za certifikát na společnost dodavatele (subdodavatele) případně výrobce nabízeného systému, ani nesmí být nahrazeno čestným prohlášením. | ANO |  |
| Dodavatel doloží zadavateli prohlášení výrobce o shodě s požadavky Vyhlášky 82/2018 Sb. ze dne 28. května 2018 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)“ k Zákonu 205/2017 Sb., „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti“ ze dne 1. srpna 2017. | ANO |  |