Příloha č. 2 specifikace Zadávací dokumentace

Č.J. SPŠE/2249/2022

Zadavatel:	Střední průmyslová škola elektrotechnická a Vyšší odborná škola Pardubice
Název veřejné zakázky:	Logmanagement

Logmanagement

Požadujeme dodat a implementovat centrální úložiště pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

Nutností je možnost procházení těchto logů integrovaným grafickým rozhraním s předdefinovanými pravidly pro rychlé vyhledávání (např. jako jsou změny v systémech provedené administrátory; seznam nově vytvořených účtů v MS AD a Office365 za zvolenou periodu; změny v přístupových právech pro zadaného uživatele nebo k zadané složce; monitoring privilegovaných účtů, sdílených účtů a změn konfigurací; sledování souborových systémů apod.) Dále musí systém umožňovat sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

Cílem je mít jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Systém musí dále umožňovat snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalostí programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.

Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný systém podporoval plánované i ad-hoc zálohování vzniklých dat na externí zálohovací systém, optimálně za využití SMB protokolu. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců – dle "Bezpečnostního doporučení NCKB pro Administrátory 4.0“. Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat.

Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině.

Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

V případě pochybností o vlastnostech nabízeného systému si vyhrazujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je uchazeč povinen dodat funkční vzorek do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále si vyhrazujeme právo vyžádat

kontakty alespoň na 3 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.

Požadujeme ocenit dedikovaný systém pro sběr, analýzu a dlouhodobou retenci logovaných událostí splňující následující technickou specifikaci:

LogManagement		
Požadavek na funkcionalitu	**Minimální požadavky**	**Nabízené parametry**
HW appliance pro zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	ANO	
Redundantní zdroje a ventilátory. Ventilátory za provozu vyměnitelné.	ANO	
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 500GB uložených událostí za den.	ANO	
CPU min. 16 jader s podporou HyperThreadingu nebo Multi-Threadingu.	1x	
Operační paměť RAM	64GB DDR-4	
Síťové rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.	4x 1GE RJ45	
Průměrný trvalý příjem událostí/s. (průměrná délka zprávy min. 700Byte)	2000 událostí/s	
Špičkový příjem bez ztráty dat po dobu nejméně 10 minut (průměrná délka zprávy min. 700Byte)	4000 událostí/s	
Čistá velikost integrované databáze	12 TB	
Příjem a zpracování logů, události a další strojově generovaná data prostřednictvím protokolů	SYSLOG (RFC3164, RFC5424, RFC5425), RELP	
Bezagentový sběr událostí, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů	ANO	
Jedna webová console pro všechny administrátorské i operátorské činnosti	ANO	
Výrobcem vytvářené parsery pro běžné systémy.	100	
Uživatelsky definované parsery - systém umožňuje dopsání parserů pro další zdroje log zařízení uživatelem pomocí tzv. vizuální programování, bez nutnosti spolupráce s výrobcem.	ANO	
Standardizace přijatých logů do jednotného formátu a jejich normalizace (rozdělení) do příslušných polí dle jejich typu. Vytvoření vlastního důvěryhodného časového razítka ke každému logu.	ANO	
Uchování originální verze přijatých logů/zpráv včetně původní časové značky události.	ANO	
Okamžitá a automatická indexace umožňující okamžité prohledávání událostí.	ANO	
Podporované formáty	RAW, Syslog (RFC5424), CEF,	

	LEEF, JSON (RFC8259)	
Systém nesmí umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. (ani libovolnou konfigurační změnou)	ANO	
Automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy	ANO	
Nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty	ANO	
Ověřování uživatele na externím LDAP serveru resp. ověření lokálního účtu v případě výpadku LDAP.	ANO	
Grafické rozhraní musí umožňovat filtraci nerelevantních událostí, snadné vyhledávání událostí, vytváření reportů a dynamickou vizualizaci událostí.	ANO	
Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů	ANO	
Uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování	ANO	
Podpora základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.	ANO	
Výrobcem předpřipravené sety/vzory alertů a korelací.	ANO	
Monitoring stavu systému - alertování při překročení prahových hodnot	SMTP nebo Syslog	
REST-API pro integraci s externím monitorovacím systémem	Zabbix, Nagios, MRTG	
Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba	ANO	
Síťové rozhraní pro management HW	1x 1GE RJ45	
Uživatelské role definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému	ANO	
Aktualizace systému přes centrální webovou správcovskou konzoli v jednom balíku.	ANO	
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.	ANO	
Podpora komprese ukládaných dat	ANO	
Podpora důvěryhodného zálohování komprimovaných dat na externí systém.	ANO	
Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce.	ANO	
Servisní podpora na HW s opravou v místě instalace serveru, s garantovanou NBD od nahlášení závady.	5 roků	
Servisní podpora na SW v rozsahu aktualizaci systému a parserů, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	1 rok	

Systémové práce musí obsahovat minimálně:

- Montáž do racku
- Připojení do LAN infrastruktury
- Napojení významných log zdrojů stávající infrastruktury
- Nastavení reportingu
- Nastavení alertů
- Zaškolení obsluhy
- Akceptační testy

V Pardubicích dne:

Mgr. Petr Mikuláš

ředitel školy