Příloha č. 3 Zadávací dokumentace

Technická specifikace Veřejné zakázky

Minimální technické požadavky na zařízení, které zadavatel požaduje:	
1	Řešení musí být dodáno jako all-in-one řešení (hardware + software).
2	Podporované protokoly: Syslog, Windows Events Collection (WinRM/RPC), FTP, S/FTP,SCP, ODBC/JDBC, log file protokol, RELP.
3	Licence pro trvalé zpracování 5000 EPS.
4	Řešení musí integrovat sběr událostí ze stávajících aplikačních zdrojů, jejichž výčet je uveden dále: NIS • IS-01 Akord, PACS • IS-02 ePACS, • IS-03 Marie PACS, LIS • IS-04 OpenLIMS, HR • IS-05 Avensio, LEK • IS-06 Lékárenský systém MEDIOX LESK od firmy Medoro s.r.o. Antivirové řešení - Eset Infrastruktura • KS-01 Active Directory • KS-01 Síťové prvky (switche, firewally, 40xWIFI AP) • KS-01 Servery a disková pole Sonda FlowMon
5	Licence pro neomezený počet zdrojů událostí připojený do SIEM.
6	Řešení nebude licenčně omezeno úložnou kapacitou.

7	Licence musí umožnit budoucí změnu architektury z All-in-One na distribuovaný systém bez dalších licenčních poplatků.
8	Licence umožňuje dočasné překročení EPS.
9	Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM.
10	Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní. Požadujeme jednotnou centrální webovou konzoli pro přístup k logům, reportům, alertům. Požadujeme jednotnou centrální webovou konzoli pro správu systému. Tato konzole musí umožňovat provádět veškeré konfigurace, správu a analýza logů.
11	Možnost definovat na základě rolí uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům.
12	Podpora šifrované komunikace mezi zdroji logů a SIEM.
13	Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů. Systém ale musí rovněž umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti externích autentizačních mechanismů).
14	Minimální administrace (výběr zařízení ze seznamu od výrobce)pro připojení dalších zdrojů událostí (Windows Active Directory Servery, Windows IIS a Exchange Servery, Windows Standalone Servery, UNIX and Linux Servery, DNS and DHCP Servery, Database Servery, Proxy Servery, Firewaly, IDS, IPS, a DAM, Routery and Switche.)
15	Zadavatel musí mít možnost řešení automaticky aktualizovat výrobcem s četností minimálně 4x ročně, a to bez dalších nákladů.
16	Řešení zahrnuje automatický Backup a následný Restore (na vyžádání obsluhy systému) Požadujeme podporu zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celé řešení.
17	Řešení musí poskytovat interní kontroly stavu zařízení (HealthCheck) a upozornit uživatele v případě problému.
18	Řešení musí poskytovat analytické a korelační funkce bez dalších zásahů a činností (out-of-the-box).
19	Řešení musí obsahovat možnost rozšíření výběrů o uživatelské položky z obsahu logů.
20	Řešení musí disponovat dostatečnou kapacitou pro ukládání dat po dobu 18 měsíců, aniž by to vyžadovalo použití externích paměťových zařízení v podobě iSCSI, NAS,

	nebo USB disků. Rozšíření kapacity zálohovacího serveru je akceptováno pouze pomocí SAS externí police.
21	Řešení musí obsahovat Near RealTime analýzu událostí.
22	Řešení musí umožňovat detekci anomálií chování uživatele vůči přistupovaným systémům a internetu.
23	Řešení musí obsahovat analýzu dlouhodobých trendů událostí.
24	Řešení musí obsahovat pokročilé "drill-down" dohledávání v případě potřeby zadavatele.
25	Řešení musí obsahovat sběr textových logů ze souborů.
26	Řešení musí obsahovat sběr logů z databází pomocí ODBC.
27	Řešení musí obsahovat vyhledávací rozhraní systému správy logů s možností rozčlenění vyhledaných dat až na detailní úroveň (alespoň IP adresa, typ události, protokol, port).
28	Řešení musí poskytovat alerty na detekované anomálie, změny chování sítě a změny v generování logů a událostí.
29	Řešení musí obsahovat fulltextové vyhledávání v nestrukturovaném textu.
30	Požadujeme automatické vytváření souhrnných informací o bezpečnostních hrozbách na základě korelace dílčích událostí.
31	Řešení musí být schopno využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu snížení false-positives.
32	Řešení musí poskytovat alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení.
33	Řešení musí poskytovat alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice.
34	Řešení musí být schopné pracovat s IP kolokacemi.
35	Řešení musí generovat alert při výpadku logů z konkrétního zařízení.
36	Řešení musí obsahovat vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server).
37	Řešení musí vyhodnocovat chybějící sekvence (např. služba přestala běžet).

38	Řešení musí být schopno korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce – zadavatele (s přesnou identifikací uživatele).
39	Řešení musí poskytovat rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy.
40	Požadujeme pravidelnou, plánovanou tvorbu reportů minimálně ve formátech PDF, případně generování ručních reportů s možností exportu ve formátu CSV.
41	Požadujeme nezměněnou funkcionalitu reportingu i při změně nebo náhradě některé technologie, jako např. firewallu nebo IDS.
42	Řešení musí podporovat vysokou dostupnost (HA) bez rozšiřujících komponent/software třetích stran.
43	HA musí být možné připojit v jakékoliv fázi, bez nutnosti reinstalace celého řešení.
44	Řešení musí podporovat downgrade, pro případ problémů s novou verzí řešení po upgrade.
45	Řešení musí poskytovat přístup k datům skrze otevřené REST API pro integraci s libovolným počtem dalších systémů.
46	Řešení musí být navrženo tak, aby bylo schopno pracovat s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti.
47	Řešení musí uchovávat logy jak v normalizovaném formátu, tak i „raw" formátu.
48	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.
49	Řešení nebude licenčně omezeno počtem generovaných reportů.
50	Řešení nebude licenčně omezeno počtem současně připojených administrátorů či operátorů.
51	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.
52	Řešení musí poskytovat zjednodušený dashboard pro operátory v českém jazyce.

Instalační a implementační práce prováděné dodavatelem:

- Instalace hardware v prostředí zadavatele
- Instalace obslužného software
- Instalace agentů, pokud jsou pro dané řešení potřeba
- Nastavení logovacích politik dle požadavků zadavatele
- Analýza a nastavení řešení pro logování sledovaných aplikací
- Nastavení síťových prvků pro sledování (konfigurace syslog)

- Nastavení serverů pro sledování
- Nastavení výstražného systému, včetně nastavení email notifikace
- Nastavení reportování
- Dokumentace celého řešení včetně postupů řešení běžných provozních situací
- Vytvoření parserů pro aplikace uvedené v rámci zadávací dokumentace
- Zaškolení obsluhy v rozsahu 3x8 hodin, a to včetně proškolení ve vytváření nových parserů v grafickém rozhraní aplikace

Budou vyžadovány tyto akceptační testy:

- Detailní parsování logů zařízení a aplikací uvedených v rámci zadávací dokumentace
- Test příjmu alespoň 4000 událostí za vteřinu, v 10 minutovém intervalu s pomocí generátoru událostí
- Test příjmu alespoň 5000 událostí za vteřinu k ověření chování řešení v situaci maximální zátěže, v 10 minutovém intervalu s pomocí generátoru událostí. Řešení musí události udržet v rámci vyrovnávací paměti.
- Vytvoření ukázkových reportů dokumentujících různé výstrahy jdoucí z podporovaných aplikací
- Ukázka vytvoření vlastního dashboardu
- Test příjmu výstrah na definovaný email

Servisní podpora řešení:

- 5 let on-site, odezva následující pracovní den od nahlášení, nahlášení možné 24x7x365