Č.j. 1/120/1902010 - 2018

Příloha č. 1 - Podrobná specifikace požadavků, služeb a cen

1. **Technická specifikace řešení**

Dodavatel vyplní všechny žlutě označené části. Tato příloha slouží **k vymezení minimálních technických požadavků zadavatele na technologii, kterou bude zajištěna služba a osvědčení jejich splnění dodavatelem**. Dodavatel vyplní všechny položky sloupce 2 (např. popisem nabízeného parametru nebo jen slovem „SPLŇUJE“, pokud by byl popis stejný jako text uvedený ve sloupci Požadavek na funkcionalitu).

**Název / typ řešení /:**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 1 | Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE |  |
| 2 | Bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém) |  |
| 3 | Licence pro zpracování 600 EPS s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 3000 EPS |  |
| 4 | Počet zdrojů pro sběr logů minimálně 165 |  |
| 5 | Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM |  |
| 6 | Možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku) |  |
| 7 | Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní |  |
| 8 | Možnost definovat uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům |  |
| 9 | Automatická identifikace systémů – zdrojů logů |  |
| 10 | Podpora šifrované komunikace mezi zdroji logů a SIEM |  |
| 11 | Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentifikace uživatelů |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 12 | Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače Cisco, hw IBM/Lenovo, Fujitsu a firewall FortiNet, Cisco FirePower) |  |
| 13 | Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí |  |
| 14 | Automatické připojení zařízení výrobců IBM/Lenovo, Fujitsu, Cisco a FortiNet |  |
| 15 | Podpora sběru síťových toků (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, sondy) |  |
| 16 | Řešení musí umožňovat automatické aktualizace |  |
| 17 | Webové uživatelské rozhraní pro management, analýzu a reporting |  |
| 18 | Poskytování automatického backup/recovery procesu |  |
| 19 | Poskytovat interní kontroly stavu zařízení řešení (healthcheck) a upozornění uživatele v případě problému |  |
| 20 | Možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI |  |
| 21 | Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box) |  |
| 22 | Řešení musí být dodáno jako all-in-one appliance (např. virtuální server) |  |
| 23 | Sběr logů z dalších bezpečnostních a síťových systémů (minimálně Cisco IOS, Cisco FirePower, FortiNet) |  |
| 24 | Výkonová rozšiřitelnost, přidáním podkladového HW |  |
| 25 | Možnost rozšíření výběrů o uživatelské položky z obsahu logů |  |
| **Požadavek na funkcionalitu** | | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 26 | Zajištění integrity nasbíraných dat |  |
| 27 | Schopnost uchovat nejméně 5 TB dat (v komprimovaném formátu), aniž by vyžadovalo použití externích paměťových zařízení |  |
| 28 | Umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware |  |
| 29 | Near-real-time analýza událostí |  |
| 30 | Analýza dlouhodobých trendů událostí |  |
| 31 | Řešení musí být hodnocené v segmentu „leaders“ v GartnerMagicQuadrantu za minulých pět let |  |
| 32 | Pokročilé "drill-down" dohledávání v případě potřeby |  |
| 33 | Možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení |  |
| 34 | Podpora a normalizace časových značek z různých časových zón |  |
| 35 | Sběr textových logů ze souborů |  |
| 36 | Sběr logů z databází pomocí JDBC/ODBC |  |
| 37 | Sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server |  |
| 38 | Rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň (IP adresa, typ události, protokol, port atd.) |  |
| 39 | Způsob zadávání vyhledávání: Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy |  |
| 40 | Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 41 | Kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně |  |
| 42 | Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy |  |
| 43 | Korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení |  |
| 44 | Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení |  |
| 45 | Alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu |  |
| 46 | Řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán). |  |
| 47 | Vykonávání akci v závislosti na přijatém logu jako např. zaslat email |  |
| 48 | Schopnost pracovat s IP geolokacemi (botnet kanály atp.) |  |
| 49 | Generování alertu při výpadku logů z konkrétního zařízení |  |
| 50 | Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server) |  |
| 51 | Vyhodnocení chybějících sekvencí (např. služba přestala běžet) |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | | **Prohlášení uchazeče zda požadavek SPLŇUJE/NESPLŇUJE** |
| 52 | Schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů |  |
| 53 | Schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele) |  |
| 54 | Schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů) |  |
| 55 | Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy |  |
| 56 | Nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS |  |
| 57 | Požadujeme automatické vytváření měsíčního reportu o stavu událostí na síti zadavatele a o všech provedených změnách prodávajícím. |  |
| 58 | Zdarma rozšíření UBA (User Behavioral Analytics) dodané vendorem s machime learning funkcionalitou. |  |
| 59 | Přístup k vendorem ověřeným (nikoliv komunitním) rozšířením, tedy aplikacím a pravidlům zdarma v rámci dodaného řešení. |  |
| 61 | Součástí dodávky je i přístup ke komerčním premiovým threat intelligence informacím a to nativní integrací. Pouze open source threat intelligence nesplňuje tento požadavek, avšak zadavatel che mít možnost takový zdroj zapojit dle vlastního výběru. |  |

1. **Služby**

Součástí dodávky musí být analýza aktuálního stavu v rozsahu minimálně 5MD, dále implementace (instalace a konfigurace) v rámci jednoho datového centra (virtualizace na platformě Hyper-V 2016) včetně integrace se 166 zdroji (viz. tabulka monitorovaných technologií). Celá dodávka bude detailně zdokumentována. Po finální implementaci dodavatel zajistí jeden měsíc pilotního provozu (zajištění vzdáleného dohledu a spolupráce na řešení jednotlivých událostí a incidentů v rozsahu 5x8 v pracovní době od 8:00 do 16:00)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Type** | | **Qty.** | **EPS Factor** | **EPS Rate** |
| Event Sources | Windows Active Directory Servers | **5** | 15 | 75 |
| Windows IIS and Exchange Servers | **2** | 10 | 20 |
| Windows General Purpose Servers | **20** | 2 | 40 |
| UNIX and Linux Servers | **30** | 0,5 | 15 |
| DNS / DHCP Servers | **6** | 15 | 90 |
| Antivirus Servers | **2** | 20 | 40 |
| Database Servers | **30** | 1 | 30 |
| Proxy Servers | **0** | 25 | 0 |
| Large Firewalls | **1** | 150 | 150 |
| Small Firewalls | **1** | 20 | 20 |
| IDS, IPS and DAM | **5** | 5 | 25 |
| VPN | **4** | 5 | 20 |
| Routers and Switches | **60** | 0,25 | 15 |
| Application Server | **20** | 3 | 60 |
| **Total Log Sources** | | **166** | **Total EPS License** | **600** |

1. **Ceny**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Položka** | **Cena v Kč bez DPH** | **Výše DPH v Kč** | **Cena v Kč vč. DPH** |
| **1.** | **Analýza** k implementaci řešení SIEM a Zpráva o implementaci řešení SIEM |  |  |  |
| **2.** | **Dodávka** řešení SIEM, včetně nezbytných SW licencí pro zajištění komplexní funkčnosti řešení SIEM ( SW Subscription & Support 12 Months) |  |  |  |
| **3.** | **Implementace** (instalace a konfigurace) řešení SIEM |  |  |  |
| **4.** | **Dokumentace** o provedené implementaci řešení SIEM |  |  |  |
| **5.** | **Pilotní provoz** – 1 měsíce, včetně zprávy o průběhu pilotního provozu |  |  |  |
|  | **Celková cena** |  |  |  |