Nástroj pro záznam a vyhodnocení logových událostí (Log Management)

**Zadání**

V rámci zvýšení kybernetické bezpečnosti bude začleněna technologie Log Managementu jako specializovaného bezpečnostního řešení, které umožňuje sbírat, parsovat, optimalizovat a analyzovat události ze všech možných vrstev IT infrastruktury.

LM řešení bude nedílnou součástí monitoringu kybernetické bezpečnosti města. Řešení Log Management, v rámci projektu, je uvažováno s konfigurovatelným uživatelským oddělením rolí s využitím silných šifrovacích metod a ochranou logů před neoprávněným přístupem k citlivým datům.

V rámci implementace požadujeme napojení všech relevantních zdrojů, jejich rozsah bude upřesněn v rámci návrhu cílového konceptu nasazení Log Managementu.

Požadujeme dodání cloudového řešení, kdy na straně města bude potřebný kolektor pro sběr logů a samotné uložení, zpracování a uchování logů bude na straně vendora případně dodavatele. Požadujeme přímý přístup k logovým záznamů minimálně v rozsahu potřebném pro jejich vyhodnocení. Dále požadujeme od dodatele servis v rozsahu nutném pro zajištění bezchybné funkce LM a sběru dat. Případně změny nebo napojení dalších zdrojů nepožadujeme zahrnout do nabídky, ale bude řešeno ve formě poptávky a nabídky ze strany zadavatele. Pro transparentnost požadujeme do nabídky uvést cenu za hodni práce servisního technika.

Ze strany dodavatele také požadujeme zajištění servisního rozhraní ve formě helpdesku pro zadávání servisních požadavků.

**Obecné vlastnosti**

Log Management bude řešením, které bude seskupovat provozní a bezpečnostní záznamy z HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity.

Požadujeme přehledné webovému rozhraní pro vyhledávání v logových záznamech, přizpůsobitelné reporty a statistiky, tak aby Log Management umožnil snazší práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

Požadované řešení bude nyní sloužit primárně jako Log Management, ale požadujeme dodání řešeni, které bude rozšířitelné o část SIEM (v rámci řešení, nebo jako další součást) s tím, že nyní bude technicky využita pouze část Log Managementu.

Požadované funkční a nefunkční vlastnosti Log Managementu

Požadujeme řešení, které umožňuje seskupovat provozní záznamy HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity. Dále požadujeme přehledné webové rozhraní pro vyhledávání, přizpůsobitelné reporty a statistiky, tak aby Log Management usnadnil práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Forma obsluhy | Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní. |
| **Počet podporovaných zdrojů log. událostí** | **500 IP adres** |
| **Komponenta Log Managementu musí mít garantovanou licenci pro:** | **Zpracování 250 EPS nebo 10 GB/day** |
| **Provedení** | **Virtuální appliance: Pro účely navrženého řešení budou zadavatelem poskytnuty zdroje na jeho virtuální platformě.** |
| Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat. | SNMP, syslog:  - UDP (dle RFC 3164),  - TCP,  - IETF (RFC 5424) + TLS |
| Aktivní sběr logů z databází. | přes ODBC, minimálně MSSQL, MYSQL, ORACLE |
| Podpora BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance. |  |
| Podpora výstupních protokolů (destinations ~ umístění log záznamů). | syslog (UDP, TCP, IETF).  zápis logových dat napřímo do databází (ODBC).  zápis logových dat do JSON formátu.  SNMP Trap. |
| Řízení přístupů (AAA) - řízení přístupu na úrovni jednotlivých úložišť (logspace). |  |
| Zálohování, Archivace, Export, Sdílení log dat | Nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace).  Nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat.  Podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru. |
| Rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů). | Velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích. |
| Možnost vyhledávání přes REST API rozhraní. |  |
| Všechny potřebné komponenty HW i SW musí být součástí dodaného systému LM, včetně databáze. |  |
| Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím MS EDGE a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X. |  |
| Systém LM musí umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD. |  |
| Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně. | Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenu strukturu a význam dat. |
| **Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup) a samostatných oddělených logspace.** |  |
| Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat. |  |
| Systém LM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat. |  |
| Komponenta sbírající logy, musí být schopna trvale zpracovávat 10000 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení. |  |
| Komponenta Log Managementu musí mít garantovaný výkon pro zpracování 10000 EPS. |  |
| Systém dále musí umožnit uchovávání logů formou záloh a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu LM. |  |
| Licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, atd). |  |
| Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů. |  |
| Vrstva sběru logů musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenu strukturu a význam dat. |  |
| Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenu strukturu a význam dat. |  |
| Vrstva sběru logů musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů. |  |
| Komponenta sbírající logy je musí posílat dále zašifrované a komprimované a musí umožňovat regulovat šířku užívaného pásma. |  |
| LM systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn dat; |  |
| LM musí ukládat data v komprimované podobě pro úsporu diskové kapacity, a to v rámci interního i externího úložiště; |  |
| LM systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu; |  |
| LM systém musí poskytovat mechanismus detekce neautorizovaných změn dat (kontrola integrity) v souborech systému LM; |  |
| Systém LM musí poskytovat reporty i ve formě grafů a tabulek. |  |
| Systém LM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších. |  |
| Systém LM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty. |  |
| Systém LM musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzn. raw-message. |  |
| Systém LM musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému. |  |
| Řešení poskytuje funkci event. managementu (práce s událostmi ve formě strukturovaných eventů) | Součástí dodávky je sada parserů pro obvyklá zařízení klasických ICT výrobců |
| Vrstva sběru (zpracování, parsování, normalizace,…) je logicky i fyzicky oddělená od centrální komponenty LM (server zajišťující uložení a vyhledávání) |  |
| **Záruka a servisní podpora** | **Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.** |