Správa logů
a SIEM

LOGmanager 1.7

Kategorie:
Bezpečnostní řešení
Sirwisa, *www.logmanager.cz*

Přihlašovatel:
Sirwisa, *www.logmanager.cz*
vývojář

Použití produktu: LOGmanager je systém pro centralizovanou správu i management událostí a logů z libovolných síťových aktivních prvků, bezpečnostních zařízení či operačních systémů a aplikačního softwaru. Je založený na databázi se škálovatelnou kapacitou a výkonným systémem pro prohledávání i prezentaci nalezených dat. Kromě bezpečnostního oddělení je přínosem i pro operační a provozní úseky, které mohou snadnou interakcí proti databázi událostí nalézt například podstatu nefunkčnosti systému, identifikovat možné závady a rychle dohledat události popisující příčinu konkrétního problému, ztráty dat nebo výpadku komunikace.

Popis produktu: Podstatou produktu je sběr všech relevantních eventů a logů organizace, jejich ukládání do centrálního zabezpečeného úložiště s předem definovanou retencí a možností prohledávat enormní množství dat v reálném čase. Výstupy prohledávání se prezentují v textové i grafické podobě s vysokou mírou interakce vzhledem k nalezeným datům. Systém umožňuje dlouhodobě ukládat data v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu a případné bezpečnostní audity.

Zajímavé vlastnosti produktu:
- Vysoký výkon – více než 5 000 eps
- Žádné licenční omezení
- Rychlá implementace
- Konektor na SQL databáze
- Uživatelsky přehledné a intuitivní ovládání
- Systém se konfiguruje a ovládá přes jednotné grafické rozhraní
- Nemožnost mazání uložených logů
- Konfigurace i vlastních reportů, dashboardů a alertů
- Běží na samostatné HW applianci
- Součástí systému je i Windows Event Center

Záruka: Pět let na hardware, rok na SW, záruku lze prodloužit za poplatek

Cena (bez DPH): 599 000 Kč