Termékismertető

Logmenedzsment
lépésről lépésre

Tudjuk, hogy meg kell felelni a naplófájlok gyűjtésével kapcsolatos biztonsági előírásoknak, de hogyan lesz a rendszerekből kinyert temérdek információból használható adat? Az ismertetőben a logmenedzsment megoldások kialakításához adunk tanácsokat.

NetIQ megoldások
- Logmenedzsment

Termékek
- Sentinel Log Manager
- Sentinel
- Compliance Manager

Az informatikai rendszerek biztonságát a naplófájlok hatékony kezelésével az alábbi három lépésben ajánlott egyre hatékonyabbá tenni.

1. lépés: Logmenedzsment
A minden informatikai eseményt rögzítő naplófájlok emberi feldolgozásra alkalmatlan halmazában, a NetIQ Sentinel Log Manager, leegyszerűsíti az események begyűjtését, a logok életciklusának kezelését és a jelentések készítését. A termék a bejövő eseményeket azonos formátumra konvertálja és ily módon a korábban manuális adategyeztetések (pl a felhasználónév, számítógép, vagy hálózati cím azonosítása a különböző forrásokból származó eseményekben) teljesen automatikussá válnak. A Sentinel Log Manager az egyszerű üzembe helyezés érdekében nagy számú beépített kollektorral és előre konfigurált jelentéssel érkezik. Számos időigényes, hibalehetőségekkel teli manuális folyamat váltható ki, a NetIQ log menedzsment megoldásának automatizált jelentéskészítő mechanizmusaival, így egyértelműen teljesíthetők a naplóállományok kezelésére és az ezekből származó adatok előállítására vonatkozó biztonsági előírások követelményei.

2. lépés: Valós idejű elemzés
A hatalmas mennyiségű adathalmaz állandó ellenőrzése és elemezhetősége szempontjából, a hangsúly az automatizáláson, az események és a megfelelőséget sértő tevékenységek azonnali automatikus kezelésén van. A NetIQ Sentinel képes a biztonsági eseményfolyam valós idejű megjelenítésére és elemzésére.

Az események ellenében incidensek nyithatóak, akciók kezdeményezhetőek, amelyek a korrelációs motor révén akár több esemény egyidejű bekövetkezéséhez is köthetőek. A Sentinel tartalmazza a Sentinel Log Manager funkcionalitását és kiegészíti azt a valós idejű elemzéssel és risztással, így nagy mértékben képes a logmenedzsment folyamatok hasznosságát fokozni.

3. lépés: Integráció IAM rendszerekkel
A biztonsági fenyegetések leküzdése, valamint a számtalan belső és külső auditálási elvárás teljesítése érdekében a vállalatok általában többféle felhasználói erőforrás-kiosztási, jogosultság- és hozzáférés-kezelési rendszert (IAM – Identity and Access Management) használnak. A fejlesztés következő lépéseként érdemes megoldani a logmenedzsment integrációját az IAM megoldásokkal. A NetIQ Compliance Management Platform integráltan tartalmazza a Novell legújabb biztonsági megoldásait, többek között az NetIQ Identity Manager személyazonosság-kezelési és a NetIQ Sentinel információbiztonsági és eseménymenedzsment megoldást is. A NetIQ Compliance Management Platform segítségével ezek a rendszerek egy olyan biztonsági megfigyelőrendszerré állnak össze, amely nemcsak biztonságosan kezeli a személyazonossági adatokat, de automatikusan, valós időben érzékeli, jelenti és orvosolja a nem megfelelő vagy gyanús tevékenységeket. A NetIQ szakértői abban az esetben is képesek a logmenedzsment és az IAM megoldás integrációjára, ha ezek közül csak az egyik NetIQ termék.

Keresse meg helyi megoldásszállítóját, vagy vegye fel a kapcsolatot a NetIQ magyarországi képviseleti irodájával az alábbi elérhetőségek valamelyikén:

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
info@netiq.hu
www.netiq.hu

NetIQ | Novell | SUSE

NetIQ