

## Ismertető

# Logmenedzsment

## lépésről-lépésre

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

A Novell szerint érdemes olyan biztonságfelügyeleti modellt alkalmazni, amely a következő, fokozatosan felépített 3 fő lépésből áll

### 1. lépés: Log menedzsment

A minden informatikai eseményt rögzítő naplófájlok emberi feldolgozásra alkalmatlan halmazában a Novell Sentinel Log Manager leegyszerűsíti az események begyűjtését, a logok életciklusának kezelését és a jelentések készítését. A termék a bejövő eseményeket azonos formátumra konvertálja és így 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 Novell 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 elemezhetőségszemponjtájából a hangsúly az automatizáláson, az események és a megfelelőséget sértő tevékenységek azonnali automatikus kezelésén van. A Novell

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. Ugyan teljes értékű eszköz lévén megállja helyét a Sentinel Log Manager nélkül is, organikus kiegészítőként nagy mértékben képesek egymás 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 Novell Compliance Management Platform integráltan tartalmazza a Novell legújabb biztonsági megoldásait, többek között az Novell Identity Manager személyazonosság-kezelési és a Novell Sentinel információbiztonsági és eseménymenedzsment megoldást is. A Novell Compliance Management Platform segítségével ezek a rendszerek egy olyan biztonsági megfigyelőrendszerre állnak össze, amely nemcsak biztonságosan kezeli a személyazonossági adatokat, de automatikusan, valós időben érzékeli, jelenti és orvosolja a nem megfelelő vagy gyanús tevékenységeket.

#### • Megoldás

Logmenedzsment megoldások

#### • Termékek

##### Logmenedzsment

Sentinel Log Manager

##### Valós idejű elemzés

Sentinel

##### Integrált megfelelőségi megoldás

Novell Compliance Manager

Keresse meg a Novell helyi megoldásszállítóját, vagy hívja a Novell helyi képviselőjét az alábbi számon:

+36-1-489-4600

email: [iroda@novell.hu](mailto:iroda@novell.hu)

#### Novell Kft.

1124, Budapest

Csörsz utca 45.

