Termékismertető

Change Guardian

A NetIQ Change Guardian az egyik legjobb eszköz a Windows és Linux rendszerekben zajló folyamatok biztonsági szempontból történő monitorozására. A beépített eszközöknél lényegesen kisebb teljesítményigénnyel és nagyobb részletességgel naplózza a fájlokhoz és könyvtárakhoz való hozzáférést, a címtárban, illetve a házirendekben történt módosításokat.

NetIQ megoldások

- Biztonsági eseménykezelés

Termékek

- Change Guardian for Windows
- Change Guardin for Unix/Linux
- Change Guardian for Active Directory

Bevezetés

A NetIQ Change Guardian termékcsaláddal valós idejű védelmet biztosíthat kulcsfontosságú fájljai és rendszerei számára. Észlelheti a felügyelet nélküli módosításokat, a kritikus adatokhoz való illetéktelen hozzáférést, az engedély nélküli, kiemelt jogosultságot igénylő tevékenységeket, ezáltal jelentősen csökkentve a bizalmas adatokra és rendszerekre leselkedő biztonsági kockázatokat, továbbá biztosíthatja az olyan adatvédelmi szabványoknak és előírásoknak való megfelelést, mint pl. a bankfelügyelet előírásai, vagy akár a PCI DSS, a HIPAA/HITECH, az ISO/IEC 27001 és az EU adatvédelmi irányelve.

A termék áttekintése

A NetIQ Change Guardian termékekkel nyomon követheti a hozzáféréseket és a módosításokat, továbbá reagálhat a felmerülő kockázatokra.

A termékcsalád a következő tagokból áll:

- **NetIQ Change Guardian for Windows** – figyeli a fájlokon, könyvtárakon, megosztásokon, a rendszerleíró-adatbázisban és a rendszerfolyamatokon végrehajtott módosításokat, azonnal jelezve, ha potenciálisan veszélyes változás történik a kiszolgálókon.

- **NetIQ Change Guardian for Unix/Linux** – figyeli a Linux és Unix rendszerek kritikus fájljain végrehajtott módosításokat, és így segít az iparági és törvényi előírások teljesítésében.

- **NetIQ Change Guardian for Active Directory** – valós időben figyeli az Active Directory szolgáltatásaiban végrehajtott felügyelet nélküli módosításokat, figyelmeztet azokra, és növeli az előírásoknak való megfelelést.

A NetIQ Change Guardian termékcsalád tagjai önállóan is használhatóak, de nagyban növelik egy meglévő biztonsági információs és eseményfelügyeleti (SIEM) megoldás hatékonyságát is. Automatizálási megoldásokkal és a NetIQ Secure Configuration Manager konfiguráció-menedzsment termékkel együtt használva a NetIQ Change Guardian termékek egy hatékony, integrált és automatizált biztonsági és megfelelőségkezelési megoldás alapvető fontosságú részei lehetnek.

A NetIQ Change Guardian termékek a következő, alapvető fontosságú védelmi szolgáltatásokat nyújtják:

- **Kiemelt felhasználók kezelése –** a kiemelt jogosultsággal rendelkező felhasználók (például adatbázis-rendszergazdák tevékenységének) nyomon követése és ellenőrzése, csökkentve a belülről érkező támadások kockázatát.
- **Valós idejű változáskövetés és riasztás –** észleli és jelenti a kulcsfontosságú fájlokon, platformokon és rendszerekben végrehajtott módosításokat, segítve a behatolások elkerülését, segít biztosítani az előírásoknak való megfelelést, a SIEM megoldásokkal együttműködve pedig részletes adatokat szolgáltat a biztonsági csapatoknak.

Legfontosabb jellemzők

- Windows, Linux és Unix rendszerek teljes körű naplózása
- A beépített audit funkcióknál sokkal részletesebb, könnyebben kezelhető adatok kisebb teljesítményigénnyel
- Önálló termékként is használható, de ideális megoldás meglévő SIEM megoldás szolgáltatásinak kibővítésére is.
- Kiemelt felhasználók monitorozása
- Valós idejű változáskövetés és riasztás
- Megfelelőség teljesítésének demonstrálása

NetIQ®

www.netiq.hu

A legfontosabb jellemzők

A NetIQ Change Guardian termékek nem csupán azonosítják a fenyegetéseket, hanem részletes jelentéseket is készítenek, így segítve a hatékony és ésszerű döntéshozatalt, csökkentve a vállalati adatok elvesztésének kockázatát. A NetIQ Change Guardian termékcsalád legfontosabb jellemzői:

- Részletes, visszakereshető jelentést ad a kiemelt felhasználók tevékenységéről a Windows, Linux és Unix alapú környezetekben.
- Lehetővé teszi egyedi definíciók létrehozását azon jól ismert, kiemelt jogosultságokkal rendelkező csoportokhoz vagy tevékenységekhez, amelyeket a szervezetnek nyomon kell követnie.
- Részletes adatokat szolgáltat a módosítások és tevékenységek mibenlétéről, időpontjáról, helyéről és módjáról, valamint a módosítást végző személyéről, beleértve a módosítás előtti és utáni állapotra vonatkozó adatokat is.
- Azonosítja a felügyelt és nem felügyelt módosításokat, utóbbiakra valós időben figyelmeztet.
- Szükségtelenné teszi a beépített naplózást, és így optimális naplózás, megfelelőség és biztonsági teljesítmény érhető el, amihez csak minimális mértékben kell módosítani a meglévő infrastruktúrát.
- A figyelmeztetési rendszer minden jelentős SIEM megoldással együttműködik, így az események az egyéb biztonságfelügyeleti eszközök adatainak fényében vizsgálhatóak, tovább csökkentve az észrevétlen behatolás kockázatát.
- A jelentéskészítő eszközök a belső és külső ellenőrzések számára is megfelelő adatokat szolgáltatnak.
- Testre szabható megoldás építhető fel belőle a legnagyobb kihívást jelentő megfelelőségi követelmények teljesítésének támogatásához, a fájlokon, rendszereken, címtárakon és objektumokon végrehajtott módosítások észlelésével, dokumentálásával és a szükséges riasztások kiadásával kapcsolatban.

Fő megkülönböztető jegyek

- Az integrált biztonsági termékválaszték segít elérni a megfelelőségi célkitűzéseket, valamint a bizalmas vállalati adatok védelmét. A NetIQ Change Guardian termékekkel a legszigorúbb megfelelőségi követelményeknek is eleget tehet, beleértve a fájlok integritásának védelmét és a kiemelt felhasználók megfigyelését.
- Többféle szerver és kliens platform széles körű támogatása, segítve az informatikai és biztonsági szakértőket a kulcsfontosságú vállalati eszközök megóvásában.
- A NetIQ Change Guardian termékek a behatolás kockázatának csökkentése érdekében átfogó jelentéseket adnak a módosításokról, feltüntetve a módosítás vagy esemény előtti és utáni értékeket. A hasznos értékek mellett minimális zajt tartalmazó részletes jelentéseket pedig egy vagy több felhasználó vagy számítógép tevékenységére lebontva határozzák meg, ezzel elősegítve a szokatlan tevékenység forrásának felderítését, illetve biztosítva a vizsgálatot végzők számára a részletes információkat.
- A NetIQ Change Guardian termékek minimális infrastruktúra-módosítás mellett nyújtanak maximális teljesítményt, emellett páratlan skálázhatóságot biztosítanak a vállalaton belül, miközben a megoldások minimális mértékben befolyásolják a hálózati alkalmazásokat, kiszolgálókat, rendszereket és folyamatokat.
- A NetIQ széleskörű és díjnyertes biztonsági szolgáltatásokkal és megfelelőségkezelési szoftvertermékkel ellátott hatékony biztonsági és megfelelőségi eszközöket biztosít a fejlett biztonsági folyamatok létrehozásához és bevezetéséhez. Ezek a folyamatok segítik az informatikai erőforrások maradéktalan kihasználásában, a megfelelőség akadályoktól mentes elérésében, valamint az egész szervezetet érintő információs biztonsági kockázatok csökkentésében.

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