Termékismertető

Sentinel

A Sentinel terméket a biztonsági előírások és a megfelelési szabályok betartásának hatékony követésére és ellenőrzésére fejlesztettük ki. A kézzel végzett megfigyelés és kockázatelemzés már kis számú megfigyelt eszköz esetén is óriási teher, a Sentinel automatizálási képességeinek segítségével azonban akár több ezer szerver, hálózati eszköz, vagy szoftvertermék is hatékonyan megfigyelhető.

Bevezetés

Az olyan technológiák például, mint a virtualizáció, a felhőalapú számítástechnika és a mobilitási megoldások megváltoztatták az üzleti tevékenységek intézésének a módját és ezen új környezet biztonságának fenntartása nehéz feladat elé állítja az adatbiztonsággal foglalkozó szakértőket.

Az általános biztonsági helyzet javításához és a megalapozottabb döntésekhez a szervezeteknek valós idejű információkra van szükségük a biztonsági események elemzéséről. Rendelkezniük kell azzal a képességgel, hogy megbirkózzanak a hatalmas mennyiségű biztonsági adat kezelésének kihívásával, hogy leküzdjék a kifinomult fenyegetéseket, és hogy biztosítsák a házirend következetes betartását. Olyan megoldásra van szükségük, amelynek a segítségével gyorsan és pontosan meghatározhatják, hogy az eseményadatok tömegében mely adatok jeleznek kritikus eseményeket és biztonsági anomáliákat.

A termék áttekintése

A NetIQ® Sentinel™ biztosítja az informatikai tevékenységek teljes körének valós idejű átláthatóságát, így elősegíti a biztonsági fenyegetések kockázatának visszaszorítását, a biztonsági műveletek hatékonyságának fokozását, valamint a házirend következetes betartását a fizikai, virtuális és felhőalapú környezetekben.

Csökkenti a hagyományos biztonsági információ- és eseményfelügyelet (SIEM) bonyolultságát, és lejjebb viszi a SIEM alkalmazásának korlátait, így minden szervezet számára elérhetővé teszi a biztonsági információkat. A NetIQ Sentinel egy hatékonyabb SIEM-megoldást bocsát a szervezetek rendelkezésére, amely valós idejű információk, rendellenesség-felismerés és a felhasználói tevékenységek megfigyelésének ötvözésével biztosít korai figyelmeztetési mechanizmust és az informatikai tevékenységek pontosabb kiértékelését.

A NetIQ Sentinel az iparág egyetlen olyan rendszere, amely problémamentesen integrálható a személyazonosság-kezeléssel, így minden környezetben képes a felhasználókat bizonyos tevékenységekhez kötni. Mindezek eredményeképpen lehetővé teszi a szervezetek számára a kritikus kockázatok könnyű azonosítását, a reakcióidő jelentős lerövidítését, valamint a fenyegetések és a biztonsági rések gyors orvoslását, mielőtt azok hatással lehetnének az üzletmenetre. A valós idejű információkra támaszkodva a Sentinel képessé teszi a szervezeteket arra, hogy védekezzenek a kifinomult fenyegetések felbukkanásával szemben, fokozzák biztonsági tevékenységük hatékonyságát, és biztosítsák a házirendek folyamatos betartását.

NetIQ megoldások

- Biztonsági események kezelése (SIEM – Securtiy Information and Event Management)

Termékek

- Sentinel™

Kiegészítő termékek

- Változás monitoring, tevékenység megfigyelés: ChangeGuardian
- Konfigurációmenedzsment: Secure Configuration Management
- Rendszergazdák monitorozása: Privileged User Management
- IAM integráció: Identity Tracking

Fontosabb képességek

- Folyamatos, 24 órás megfigyelés
- Naplófájlok és események automatikus összegyűjtése, normalizálása, korrelálása
- Rendellenességek, trendek, behatolási kísérletek automatikus felismerése
- Azonnali automatikus válaszlépések az incidensekre a gyors elhárítás érdekében
- Integráció a személyazonosság-kezelő megoldásokkal, az események felhasználókhoz rendelése
- Grafikus kezelőfelület, az események grafikonok segítségével történő áttekintése
- Valósidejű riportkészítés az előírásoknak való megfelelés dokumentált bizonyításához
- Beépített hibajegykezelés, illetve együttműködés külső rendszerekkel

Fontosabb előnyök

- Robusztus, jól skálázható SIEM megoldás vállalati vagy kormányzati felhasználók számára
- A ma piacon lévő legerősebb monitorozó rendszer a PCI-DSS szabványoknak történő megfeleléshez
- Kiválóan illeszkedik a NetIQ piacvezető személyazonosság-kezelési megoldásaihoz

NetIQ®

„Noha naponta akár 35 súlyos biztonsági eseménnyel is foglalkoznunk kellett, a Sentinel lehetővé tette ezek korai felismerését és gyors orvoslását, így az események semmilyen hatással nem voltak a játékok lefolytatására.”

Vladan Todorovic, az Ifjúsági Olimpiai Játékok IT biztonsági igazgatója, Atos Origin

www.netiq.hu

Képességek és szolgáltatások

- **Rendellenesség-felismerés** – Gyakran nem egyszerű az olyan események azonosítása, amelyek valós vagy potenciális veszélyt jelentenek, és kivizsgálásra szorulnak. A Sentinel rendellenességet felismerő funkcióival automatikusan azonosítani lehet egy szervezet környezetében a felmerülő következetlenségeket, és nem feltétlenül kell kialakítani bonyolult korrelációs szabályokat. A Sentinel bevezetésekor először meghatározzák az adott szervezet környezetére vonatkozó alapértékeket, így azonnal intelligensebb módon és gyorsabban észlelheti a rendellenes tevékenységeket.
- **Rugalmas telepítési lehetőségek –** A Sentinel a jelentősebb hipervizorokra (VMware, HyperV, XEN) ISO-lemezképből, szoftverkészülékként is telepíthető, de SUSE Linux Enterprise Server és Red Hat Enterprise Server rendszeren normál alkalmazáskénti is üzembe helyezhető.
- **Egyszerűbb szűrés, keresés és jelentéskészítés** – A Sentinel leegyszerűsíti az informatikai infrastruktúra eseményeinek begyűjtését a fáradtságos megfelelőségi felülvizsgálatok és jelentéskészítési funkciók automatizálásához, és jelentősen lecsökkenti az auditorok által megkövetelt adatok kikeresésére és előkészítésére szánt időt és költséget. Ennek köszönhetően a szervezetek gyorsabban alkalmazkodhatnak a kormányzati rendeletekhez és az iparági követelményekhez.
- **Továbbfejlesztett és bővített, használatra kész jelentések** – A Sentinel adatösszesítési és normalizálási képességekkel, előre összeállított jelentésekkel, testre szabható házirendekkel és gyors keresési képességekkel egyszerűsíti le a jelentéskészítés folyamatát. Menet közben, egyetlen gombnyomással is létre lehet hozni valós idejű keresési eredményeken alapuló jelentéseket, így azonnal jelentés készíthető a kívánt adatokról, és nem kell egy behatárolt, előre összeállított sablon módosításával bajlódni.
- **Nagy teljesítményű tárolási architektúra** – A Sentinel hatékony, fájlalapú eseménytárolási megoldást használ, amelyet a hosszú távú eseményarchiválásra optimalizáltak. Az eseménytár 10:1 arányú tömörítést alkalmaz, és teljes mértékben támogatja a gyors, indexelt kereséseket. A termék lehetőséget biztosít arra, hogy a szervezet eseményadatainak egy részét vagy egészét egy relációs adatbázisba szinkronizálja, vagy akár áthelyezze oda az adatokat. A Sentinel tárolási architektúrája mellett nincs szükség külső adatbázis licencének beszerzésére, így csökkenthető a teljes birtoklási költség. A NetIQ iparágvezető felhasználói tevékenység-megfigyelési képességeket is kínál, amelyek a személyazonosság-kezelés segítségével összekapcsolják a felhasználókat a különböző rendszerekben végzett tevékenységekkel.
- **Grafikus szabálykészítő –** A NetIQ Sentinel gyorsan készíthet korrelációs szabályokat az adott környezetben gyűjtött események felhasználásával anélkül, hogy a rendszergazdáknak külön képzésen kellene részt venniük, vagy meg kellene tanulniuk egy saját parancsnyelvet. A szabályokat telepítés előtt tesztelni is lehet, így csökkenthető a téves riasztások gyakorisága, és még jobban észlelhetők a sebezhető rendszereket kihasználó támadások. Mindennek köszönhetően jelentősen lerövidíthető a megtérülési idő, a teljes birtoklási költség pedig alacsonyabb lesz.
- **Személyazonosságok alkalmazása –** A NetIQ Sentinel azonnal integrálható a NetIQ® Identity Manager rendszerrel, így az iparág egyetlen zökkenőmentes személyazonosság-kezelési integrációját biztosítja, amely a felhasználókat a vállalaton belüli adott tevékenységekhez köti. Ha kiegészítjük a biztonsági adatokat a felhasználók és rendszergazdák egyedi személyazonossági adataival, akkor sokkal részletesebb betekintést nyerhetünk abba, hogy melyik felhasználó hol és mikor fért hozzá a rendszerhez.

Fontosabb előnyök

- Virtuális szoftverkészülékként gyors és könnyű telepítést és rugalmas bővíthetőséget biztosít.
- A személyazonossági adatok alkalmazásával kontextusba lehet helyezni a biztonsági eseményeket, így jobb betekintéssel azonosíthatók és előzhetők meg a fenyegetések.
- A kiegészítő termékek (ChangeGuardian, Privileged User Manager, Secure Configuration Manager, Identity Manager) segítségével olyan extra adatok kerülnek a naplóállományokba, amelyek megkönnyítik a biztonsági incidensek azonosítását.
- A grafikus szabálykészítési felületek leegyszerűsítik az adminisztrációt. A rendszergazdák a telepítés során gyorsan kifejleszthetik a korrelációs szabályokat, és azokat könnyen frissíthetik, ha a vállalkozás változásai ezt szükségessé teszik.
- A biztonsági információk műszerfalai szinte közvetlenül a telepítés után megkezdik a szervezet biztonságának megfigyelését, így a rendszer már a legelső pillanattól értéket termel.
- Az intuitív adatkeresés lehetővé teszi a biztonságért felelős szakembereknek, hogy gyorsan kikereshessék és jelentésbe foglalhassák a szükséges adatokat.

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