Termékismertető

Privileged Account Manager

A belső fenyegetések különösen akkor jelentenek veszélyt, ha olyan alkalmazottakhoz kapcsolódnak, akik a szükségesnél magasabb szintű hozzáférési jogosultságokkal rendelkeznek. Akár az alkalmazottak saját jogosultságaikkal való visszaéléséről van szó, akár arról, hogy egy bűnöző belső hitelesítési adatok használatával fér hozzá informatikai hálózatához, a veszély úgy kezelhető a leghatékonyabban, ha szorosan ellenőrzi és figyeli a kiemelt felhasználók tevékenységét.

Rendszergazdai fiókok

A **NetIQ® Privileged Account Manager** használata esetén szükségtelenné válik, hogy a root fiókok hitelesítési adatait az összes rendszergazdának megadja. A szoftver a rendszergazda hozzáférést központi házirend alapján delegálja. E házirendek kialakítása során átfogó „ki?, mit?, hol?, meddig?” típusú modell segítségével engedélyezi vagy tagadja meg a felhasználói tevékenységet, amely a felhasználónév, a beírt parancs, az állomásnév és az időpont vizsgálatára terjed ki. A jogosultságok ilyen módon történő kezelésével felügyelheti a felhasználók által futtatható parancsok listáját, valamint azok kiadásának lehetséges idejét és helyét.

Jelszószéf

A **NetIQ Privileged Account Manager** része az Enterprise Credential Vault, egy titkosított „jelszótároló”, amely biztonságos tárolást tesz lehetővé a rendszer, az alkalmazások és az adatbázisok jelszavai számára. Az Enterprise Credential Vault segítségével központilag kezelheti a szervezet kiemelt fiókjait, valamint intuitív felületet biztosít a kiemelt felhasználóknak a jelszavak kivételére és visszaadására. A szoftver a kiemelt fiókok szélesebb körű támogatását teszi lehetővé egyes alkalmazások (például az SAP-rendszer), adatbázisok (például az Oracle DBMS) és felhőalapú szolgáltatások (például a Salesforce.com) számára.

Szabályok létrehozása

Az iparágban egyedüliként grafikus, egérrel kezelhető felülettel rendelkező **NetIQ Privileged Account Manager** leegyszerűsíti a szabályalkotási eljárást, és szinte teljesen kiküszöböli az összetett, egyes szállítókhoz kötődő, manuális parancsfájlírást. A beépített tesztelési csomag alkalmazásával a bevezetés előtt modellezheti és kipróbálhatja az új szabálykombinációkat.

Kockázatkezelés

A **Privileged Account Manager** egy egyedi kockázatelemző motor segítségével elemzi az egyes parancsokat azok begépelése közben, majd a kiadott parancs, a parancs kiadójának neve és a kiadás helye alapján 0-tól 9-ig terjedő kockázati szintet rendel hozzá. A magas kockázati szintű parancsok vörös, az alacsony kockázati szintűek pedig zöld színkódot kapnak. A köztes értékek változó színárnyalatban jelennek meg a biztonsági kockázatot jelentő események azonnali azonosíthatósága érdekében.

Tevékenységek rögzítése

Az auditorok a visszajátszási funkciókkal ellátott intuitív kezelőfelületen, egy videó formájában, minden rögzített billentyűleütési műveletet megtekinthetnek. Amennyiben egy adott esemény további vizsgálatot tesz szükségessé, azt a munkafolyamat a megfelelő vezetőkhöz irányítja, így lehetőség van az azonnali intézkedésre.

NetIQ megoldások

- Hozzáférés-felügyelet

Termék

- Privileged Account Manager

Támogatott technológiák

- **Super User Privilege Management (SUPM):** A szoftver segítségével a vállalatok gondoskodhatnak arról, hogy a kritikus parancsokat a kiemelt felhasználók a saját nevükben, és ne egy általános „rendszergazda” felhasználó nevében hajthassák végre, továbbá pontosan szabályozhatják, hogy ki milyen parancs végzésére jogosult.
- **Shared Account Password Management (SAPM):** A megoldás magában foglal egy titkosított, megerősített jelszóval védett „széfet” a személyazonossági információk, belépési kulcsok és egyéb titkos adatok tárolására.
- **Privileged Session Management (PSM):** A megoldás képes rögzíteni az egyes tevékenységeket, illetve lehetővé teszi, hogy az informatikai szakemberek távolról is ellenőrizzék, vagy valós időben monitorozzák a műveleteket.
- **Application to Application Password Management (AAPM):** Az SAPM eszközre épülve a szoftver azt is lehetővé teszi az informatikai szakemberek számára, hogy kiiktassák a konfigurációs fájlokban tárolt kódolt jelszavakat, illetve kulcsokat, és ehelyett a „széfből” hívják le a személyazonossági adatokat.

NetIQ®

Automatikus beavatkozás

A **Privileged Account Manager** kiterjesztett kockázatalapú műveletvezérlőjének köszönhetően automatizálttá válik a házirendek betartatása a kiemelt felhasználók munkafolyamatai során. Ha egy felhasználó kockázatos műveletet hajt végre, például korlátozott hozzáférésű adatokat ér el, vagy leállít egy szolgáltatást, akkor egy rendszergazda konfigurálhatja a **Privileged Account Manager** szolgáltatást úgy, hogy az automatikusan szétkapcsolja a munkafolyamatot, vagy visszavonja a felhasználó kiemelt fiókokhoz való hozzáférését.

Képességek

- A kiemelt felhasználói hozzáférések ellenőrzése és figyelése.
- Egy pontból, központilag felügyelheti a biztonsági házirendeket.
- Folyamatosan támogathatja a belső házirendek és a külső szabályozások betartását.
- A központi irányítás révén a teljes környezetben következetes házirend érvényesíthető.
- Lehetővé teszi, hogy a hozzáférési intézkedések betartatása, elemzése és a jelentéskészítés az adatvédelmi törvényeknek és előírásoknak megfelelően történjen.

Szolgáltatások

Egyetlen helyről tervezheti meg, konfigurálhatja, tesztelheti és vezetheti be a kiemelt fiókok felügyeletére szolgáló megoldást a teljes környezetben.

- Az Enterprise Credential Vault szolgáltatás biztosítja a biztonságos jelszótárolást
- Adatbázisokhoz kapcsolódó kiemelt fiókok megfigyelése.
- A kockázatalapú munkafolyamat-vezérlés automatikus munkafolyamat-megszakítást vagy hozzáférés-megvonást tesz lehetővé
- Munkamenetek távoli létrehozása és ellenőrzése operációs rendszerekhez
- Kockázatmeghatározás a magas kockázatot jelentő felhasználók gyors azonosítására
- A potenciális veszélyek elemzésére épülő, intelligens kockázatértékelés
- A billentyűleütések naplózása révén a teljes felhasználói tevékenység megfigyelhető
- Teljes körű megfelelőség-kezelést és hatósági vizsgálatot lehetővé tevő, átfogó felügyeleti képességek

Fő megkülönböztető jegyek

Az elérhető legátfogóbb felügyeleti jelentés készíthető el. A **NetIQ Privileged Account Manager** segítségével a felhasználói tevékenység teljes körűen felügyelhető, amelynek keretében mindenre kiterjedő billentyűleütés-naplózás és videórögzítés történik a teljes hitelesítő adatokon alapuló környezetben, beleértve az alkalmazásokat (például az SAP-rendszer), az adatbázisokat (például az Oracle DBMS) és felhőalapú szolgáltatásokat (például a Salesforce.com) is.

Adott hozzáférési események esetében az auditorok a billentyűleütések szintjéig tudják visszakövetni a teljes eseményt, színkódos, soronkénti részletezettség mellett, így rendelve „jogosult” vagy „jogosulatlan” állapot-megjelölést minden egyes eseményhez.

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