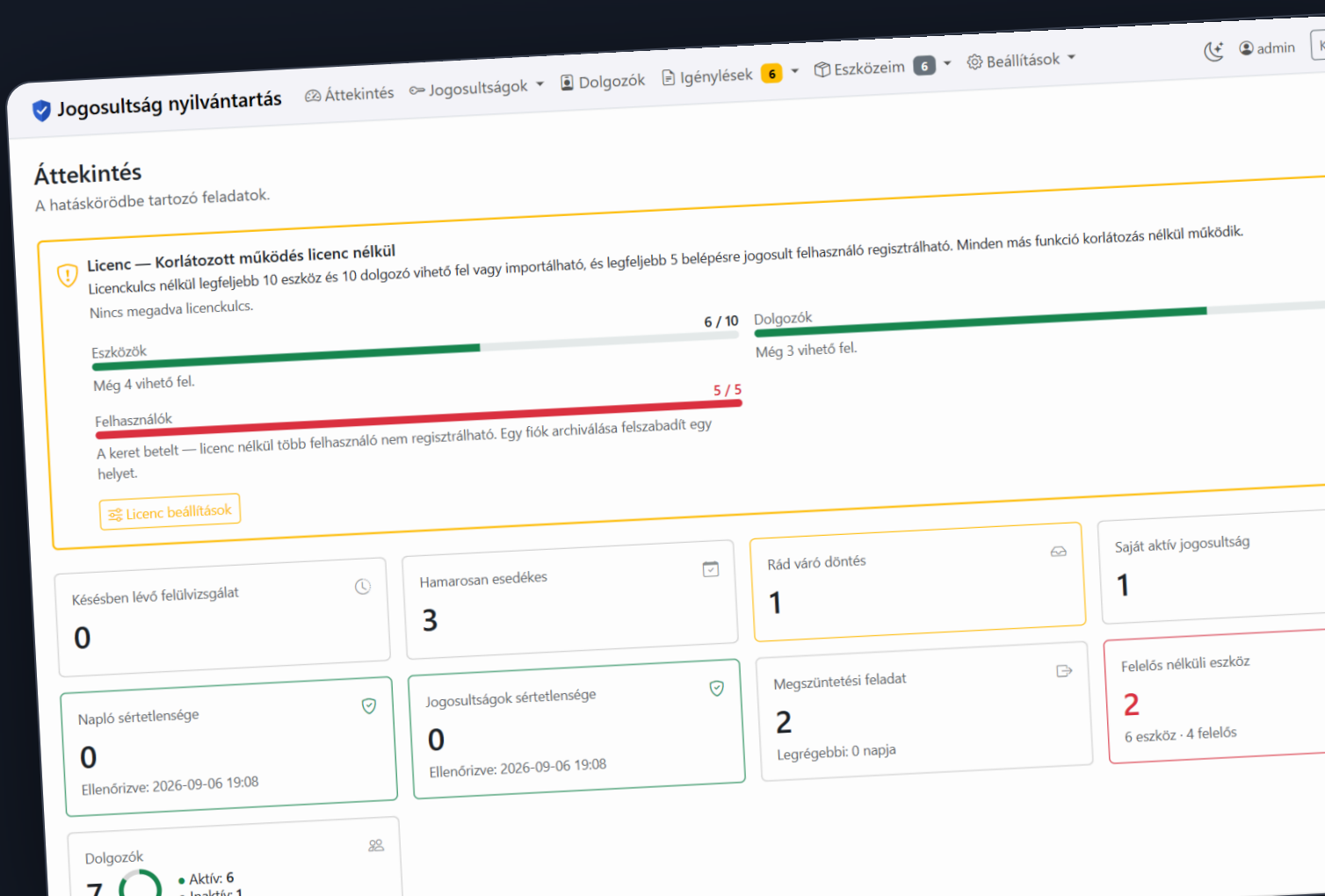
JOGOSULTSÁG-NYILVÁNTARTÁS · NIS2

devnullsec
Borics Krisztián e.v.

Minden hozzáférés mögött ott a döntés, és bizonyítani is tudod.

A Jogosultság-nyilvántartó rendszer az igényléstől a valódi rendszerből történő eltávolításig követi végig minden jogosultság életét, HMAC-pecséttel lezárt audit-naplóval, hogy a következő auditon ne magyarázkodnod kelljen, hanem megmutatnod.

- Igénylés és jóváhagyás
- Időszakos felülvizsgálat
- Megszüntetési feladatok
- Hiteles audit-napló



MIÉRT VAN RÁ SZÜKSÉG

Az Excel-táblázat nem bizonyíték.

A NIS2 nem azt kérdezi, hogy van-e jogosultsági listád, hanem azt, hogy ki döntött az egyes hozzáférésekről, mikor nézte át valaki utoljára, és tényleg megszűnt-e a kilépő kolléga hozzáférése a valódi rendszerben is. Egy kézzel vezetett táblázat ezekre a kérdésekre csak ígéretet ad, a rendszer viszont bizonyítékot.

5

szakasz, egy idővonalon

Igénylés, jóváhagyás, aktív jogosultság, felülvizsgálat és megszűnés, mindegyik névvel és dátummal.

6

megszűnési ok, automatikusan

Lejárat, kilépés, fióklezárás vagy eszköznyugdíjazás esetén a rendszer magától visszavon, és feladatot nyit.

30'

percenkénti háttérsöprés

A lejáró és esedékes jogosultságok emberi beavatkozás nélkül is a megfelelő ágra kerülnek.

Amit a rendszer a NIS2 jogosultságkezelési elvárásaiból lefed

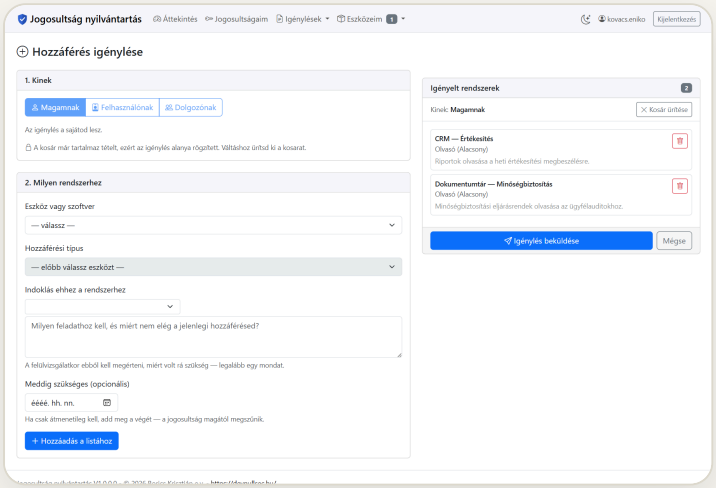
- ✓ **Eszközkatalógus** felelőssel, helyettessel és kritikussággal minden olyan rendszerhez, amihez belépni kell.
- ✓ **Igénylés és jóváhagyás** indoklással, összeférhetetlenségi szabállyal, hogy senki ne bírálja el a saját ügyét.
- ✓ **Jogosultsági és eszköz mátrix** mindig naprakészen, Excelbe exportálva.
- ✓ **Időszakos és kampányszerű felülvizsgálat** az eszközfelelősök feladatlistáján.
- ✓ **Megszüntetési feladatlista**, amely addig nyitva marad, amíg a hozzáférést a valódi rendszerből is el nem távolították.
- ✓ **HMAC-pecsétes audit-napló**, amelynek sértetlensége bármikor, akár az auditor szeme láttára is ellenőrizhető.
- ✓ **Kritikus biztonsági események** azonnali jelzése: MFA-szabály változása, integritássérülés, letiltott IP-cím.
- ✓ **Alvállalkozók kezelése** cégenként, szerződéslejárattal összekötve.

> Egy auditon az derül ki, hogy a nyilvántartást használják-e, vagy csak vezetik. Ez a rendszer az előbbire készült.

EGY JOGOSULTSÁG ÉLETE

Az igényléstől a tényleges eltávolításig.

1	2	3	4	5
Igénylés	**Jóváhagyás**	**Aktív**	**Felülvizsgálat**	**Megszűnés**
magamnak, kollégának vagy dolgozónak	a jóváhagyó dönt, indoklással	a mátrixban, HMAC-pecséttel	marad vagy visszavonás	feladat, amíg a valós rendszerben él



Kosárszerű igénylés: egy személynek több rendszer egyszerre, tételenként saját indoklással.

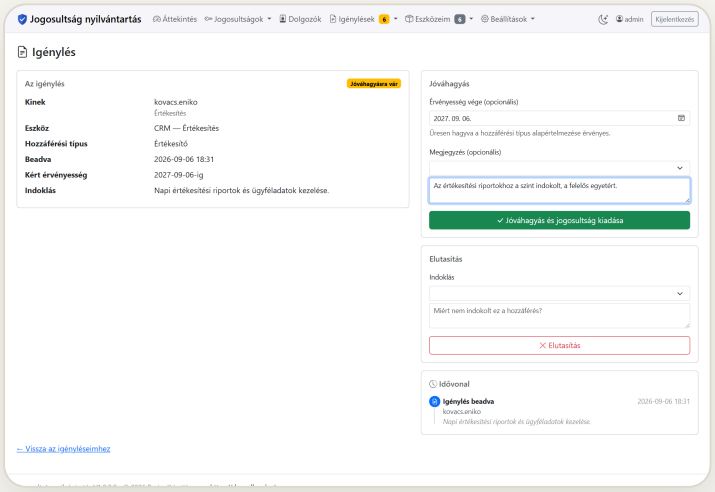
Igénylés, ami fél év múlva is érthető

Az igénylő egy kosárba gyűjti egy ember teljes belépési csomagját, a jóváhagyó pedig egyben látja, mekkora hozzáférést ad. A háttérben rendszerenként külön igénylés születik, így egy elutasítás nem viszi magával a többit.

- ✓ Kötelező indoklás, sablonokkal gyorsítva
- ✓ Határidős hozzáférés, ami magától lejár
- ✓ Fiók nélküli dolgozóknak és alvállalkozóknak is igényelhető
- ✓ Az igénylés alanya a kosárban rögzül, nem cserélődhet el véletlenül

Döntés egyetlen képernyőn

A jóváhagyási sor a bejelentkezett jóváhagyó elbírálható tételeit mutatja. A saját és a rá vonatkozó igényléseit a rendszer eleve kizárja, a jóváhagyás pedig azonnal kiadja és a mátrixba is beteszi a hozzáférést.

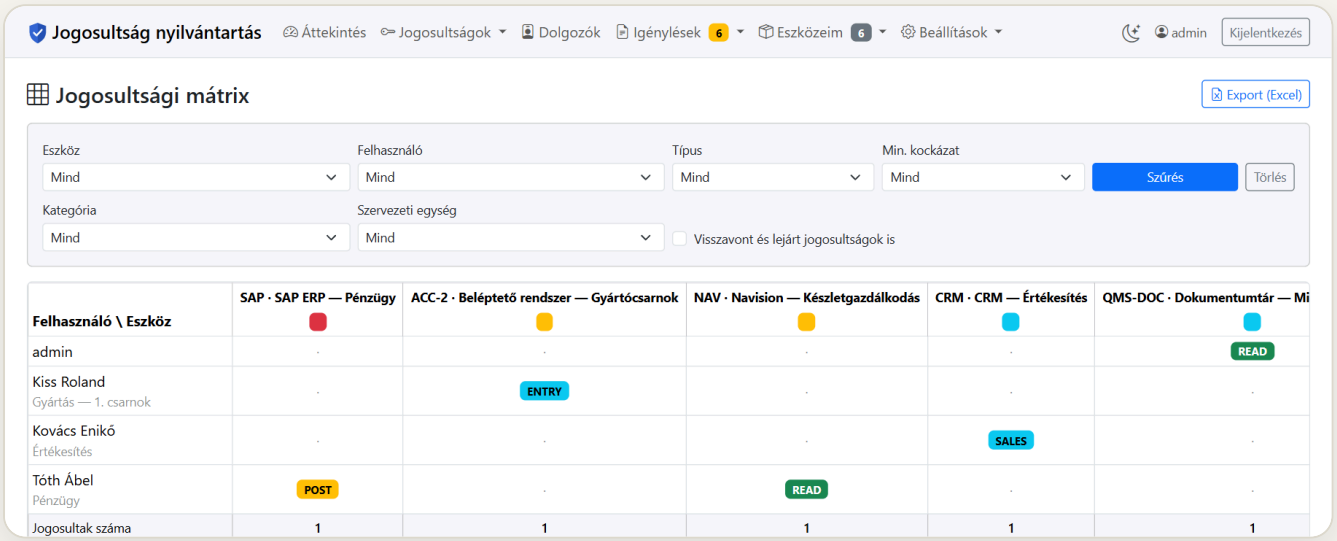


Elbírálás érvényességi dátummal és megjegyzéssel.

ÁTLÁTHATÓSÁG

Egy pillantás, és látod, ki mihez fér hozzá.

A jogosultsági mátrix felhasználókat és eszközöket feszít ki egymás ellen, kockázati színekkel. Az eszköz mátrix pedig azt mutatja meg, ki felel az egyes rendszerekért, és hol hiányzik a helyettes. Mindkettő szűrhető, és egy kattintással Excelbe exportálható.

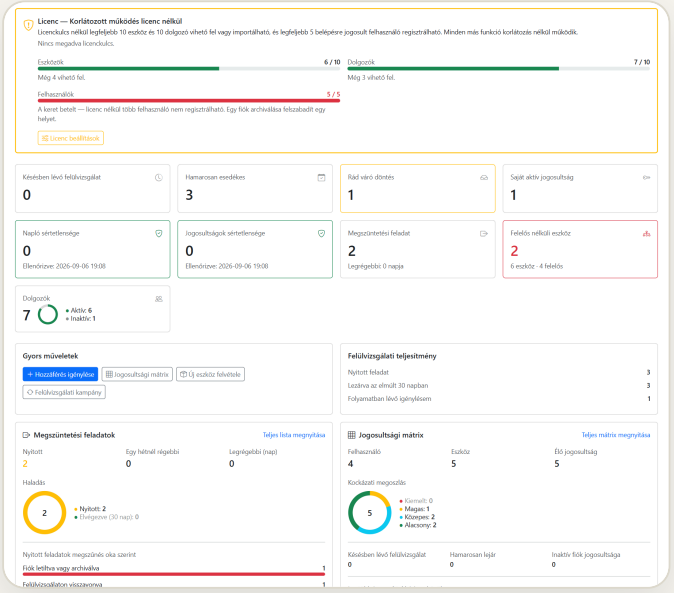


Jogosultsági mátrix: a piros keret késésben lévő felülvizsgálatot, a homokóra hamarosan lejáró hozzáférést jelöl.

Reggeli öt perc az Áttekintésen

A személyre szabott irányítópult csak azokat a kártyákat mutatja, amelyekhez az adott felhasználónak feladata van: rá váró döntések, késésben lévő felülvizsgálatok, nyitott megszüntetési feladatok és a két sértetlenségi jelző.

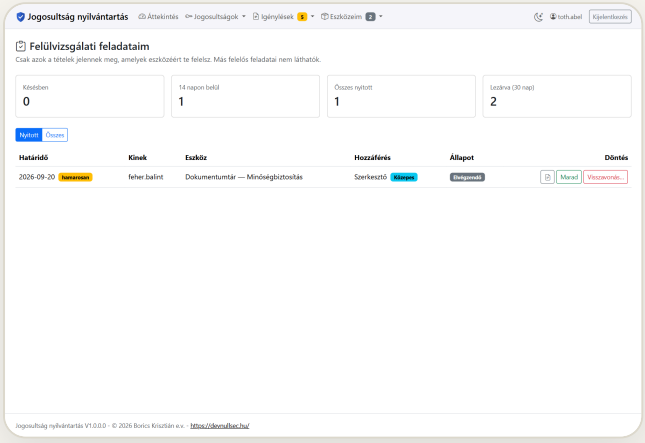
- ✓ Need-to-know szűrés minden nézetben
- ✓ Felelős nélküli eszközök kiemelése
- ✓ Belépett felhasználók élő listája



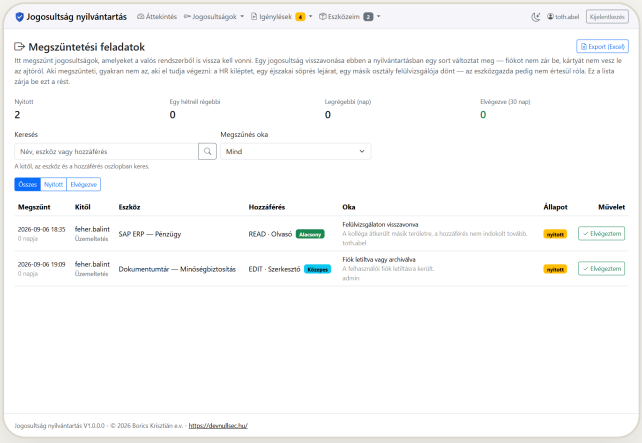
FOLYAMATOS KONTROLL

A visszavonás nem egyenlő az eltávolítással.

A legtöbb nyilvántartás ott áll meg, ahol a valódi kockázat kezdődik: egy sor átírásánál. Itt a visszavonás megszüntetési feladatot nyit az eszközfelelősnek, és a hozzáférés csak akkor számít megszűntnek, amikor valaki ténylegesen eltávolította az AD-ből, az ERP-ből vagy az alkalmazásból.



Felülvizsgálat az eszközfelelős szemével: „Marad” egy kattintás, a visszavonás mindig indoklást kér.



Nyitott megszüntetési feladat: egy felülvizsgálaton visszavont SAP-hozzáférés, ami még vár az eltávolításra.

Recertifikáció, ami körbeér

Az eszköz kritikusságához igazított időközönként a feladat magától megjelenik a felelős listáján. Átszervezés után soron kívüli kampány indítható egy eszközre vagy a teljes katalógusra.

Hat ok, egy lista

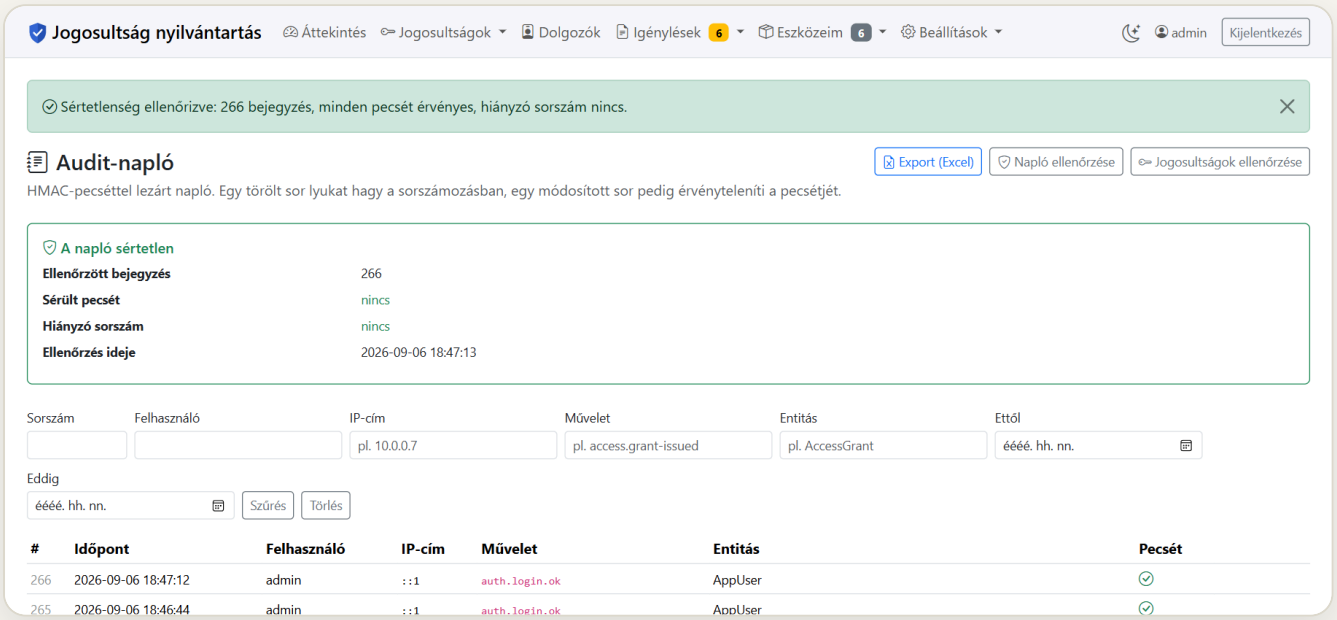
Kézi visszavonás, lejárat, felülvizsgálati döntés, fióklezárás, dolgozói kilépés vagy eszköznyugdíjazás: bármelyik történik, az eszközfelelős értesül, és a lezárás megjegyzése bekerül a naplóba.

> Az automatikus lezárás csak annyit bizonyítana, hogy a program lefutott. Az emberi lezárás azt állítja, hogy valaki megnézte.

HITELESSÉG

A nyilvántartás, ami észreveszi, ha hozzányúltak.

Minden igénylés, döntés, visszavonás és beállításváltás HMAC-pecséttel kerül az audit-naplóba. Egy törölt sor lyukat hagy a sorszámozásban, egy módosított sor érvényteleníti a saját pecsétjét, és ezt a rendszer egyetlen gombnyomásra újraszámolja.



Integritás-ellenőrzés: 266 bejegyzés, minden pecsét érvényes, hiányzó sorszám nincs.

Kötelező MFA

Globális kapcsoló a hitelesítő alkalmazásos kétlépcsős azonosításhoz, egyszer megjelenő helyreállítási kódokkal.

Titkosított mezők

Nevek, e-mail címek és TOTP-kulcsok mezőszintű titkosítással, kezelt kulcsforgatással és kulcsmegsemmisítéssel.

Kettős fék

Fiókzár öt hibás próbálkozás után, IP-tiltás tíz után, rövid tétlenségi idő és csendes munkamenet-hosszabbítás.

SZERVEZET

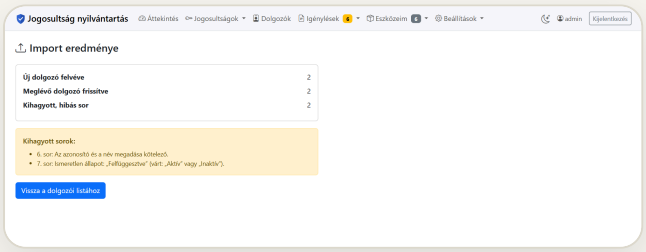
Mindenkinek pontosan annyi, amennyi kell.

Hat szerepkör, fiókonként pontosan egy. Így a „mit tehet ez az ember?” kérdésre egyetlen pillantás a válasz, és nem kell jogokat összeadni.

Szerepkör	Mit tehet
Felhasználó	Igényel magának és a fiók nélküli dolgozóknak, eszközfelelősként felülvizsgál.
Kulcsfelhasználó	Fiókkal rendelkező kollégák nevében is igényel, de nem bírál el.
Jóváhagyó	Elbírál, visszavon, és mindkét mátrixot látja.
Adminisztrátor	Katalógus, felhasználók, beállítások, audit-napló, kulcsok és kampányok.
HR	Kizárólag a saját dolgozói névsort tartja karban.
Alvállalkozói HR	Egyetlen partnercég névsorát kezeli, mást nem lát.

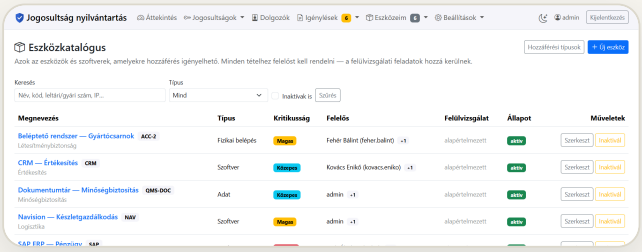
Dolgozói névsor Excelből

Nem kell minden dolgozónak fiók: a HR Excelből importálja a névsort, és a vezetők a fiók nélküli kollégáknak is igényelhetnek. Az inaktívra állított dolgozó jogosultságai azonnal megszűnnek.



Alvállalkozók szerződéshez kötve

Partnercégenként külön névsor, saját HR-fiókkal. Ha lejár a szerződés, a napi söprés a céget, a dolgozóit és minden hozzáférésüket lezárja, a cég neve pedig végig ott áll az igénylésen, a mátrixban és az exportokban. Az alvállalkozói létszám nem fogyaszt licenckeretet.



Eszközkatalógus típussal, kritikussággal, felelőssel és felülvizsgálati ciklussal.

AUDITRA KÉSZEN

Ne állítsd, hogy rendben van. Mutasd meg.

Az auditor jellemzően kiválaszt néhány élő jogosultságot, és végigköveti a keletkezésüktől. A rendszerben erre egyetlen képernyő van: a jogosultság idővonala, minden lépésnél névvel és dátummal. A leletet pedig négy rétegben, exportálható formában adod át.

Állapot

Ki mihez fér hozzá most? Mindkét mátrix Excelben.

Folyamat

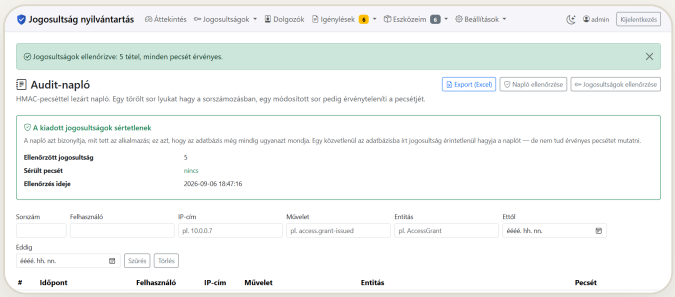
Ki döntött, mikor, mi alapján? Igénylések és felülvizsgálatok.

Napló

Hiteles-e a nyilvántartás? Pecsétes audit-napló exporttal.

Konfiguráció

Milyen szabályok szerint működik? Beállítások és kulcsleltár.



A legerősebb pillanat

Futtasd le az integritás-ellenőrzést élőben, az auditor előtt, a naplóra és a kiadott jogosultságokra is. Ez a különbség aközött, hogy állítod a nyilvántartás sértetlenségét, és aközött, hogy ott helyben bizonyítod.

Kipróbálható licenc nélkül

Licenckulcs nélkül 10 eszközzel, 10 dolgozóval és 5 felhasználóval minden funkció korlátozás nélkül működik, így a bevezetés kockázat nélkül kezdhető.

Tegyük rendbe a hozzáféréseidet a következő audit előtt.

Kérj bemutatót, és egy órában végigvesszük, hogyan illeszkedik a rendszer a szervezeted működéséhez, a katalógus felállításától az első felülvizsgálati kampányig.

devnullsec.hu