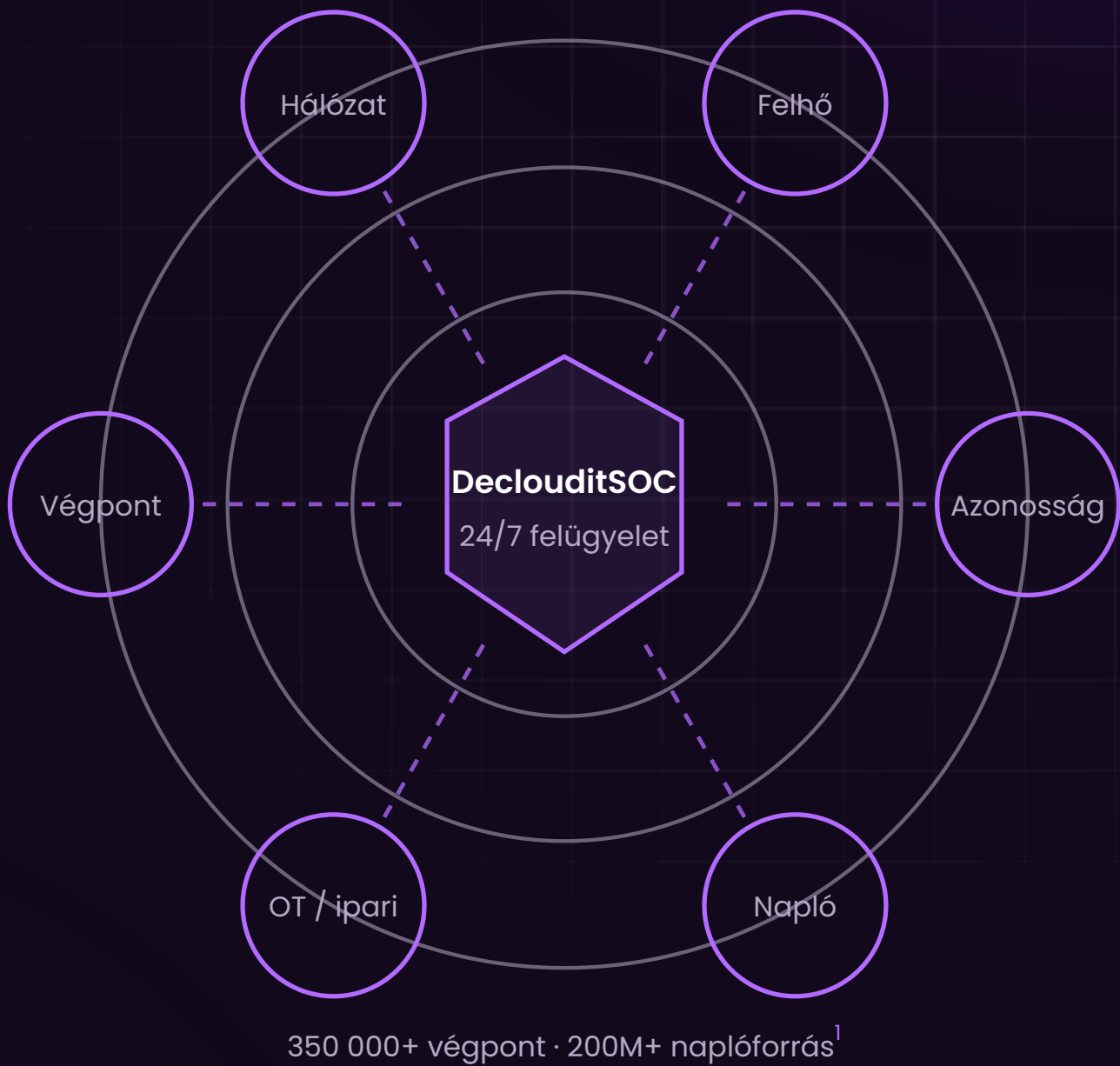


KIBERBIZTONSÁGI ÜZEMELTETÉS

Melyik riasztás igazi? Nem Önnek kell eldöntenie.

Felügyelt kibervédelem: a Decloudit 24/7 figyeli, osztályozza és lezárja a riasztásokat, mielőtt azok Önökhöz jutnának.



- Adatközpont az EU-n belül, Frankfurtban
- SOC 2 · ISO 27001 · ISO 22301 · GDPR megfelelés
- L1 szint 24/7, kritikus eseménynél L2 szakértői csapat
- Technológiafüggetlen: a meglévő eszközök naplói is bekötve

24/7

Menedzselt SOC

Frankfurt · EU

¹ A DeclouditSOC–ot a Cyrebro SOC–platformja működteti; a nagyságrendi adatok a platform gyártói adatai.

A bevezetéstől az éles üzemig

Egy támadást átlagosan 183 nap múlva vesznek észre, és még 64 nap, mire lezárják — 247 nap, mire vége.¹ A menedzselt SOC nem egy eszköz bekapcsolása: a bevezetés méréssel kezdődik, és akkor élesedik, amikor a riasztások valóban az Önök környezetéről szólnak.

BEVEZETÉS

- 1

Felmérés

1. hét

Milyen rendszerek vannak, mi a védendő üzleti érték, melyik eszköz milyen naplót ad. Ebből lesz a bekötési terv.
- 2

Naplóforrások bekötése

2–3. hét

Végpont, hálózat, felhő, azonosság, kiszolgálók — és ahol van, OT/ipari környezet. Technológiafüggetlen: a már megvett eszközök is bekötve.
- 3

Használati esetek beállítása

3–4. hét

Mi számít riasztásnak az Önök működésében. A hamis riasztás nem statisztika, hanem munka, ezért a hangolás a bevezetés része.
- 4

Próbaüzem

4–6. hét

Éles forgalmon figyelünk, de a beavatkozás még egyeztetéssel történik. Itt derül ki, mi zajos és mi hiányzik.
- 5

Éles 24/7 üzem

folyamatos

L1 szint folyamatosan, kritikus eseménynél L2 szakértői csapat. Havi jelentés, incidens után utókövetés.

MIT NYÚJTUNK

- Folyamatos figyelés** — a platform éjjel-nappal gyűjti és összefűzi az eseményeket, emberhez csak a valódi riasztás jut el.
- Elvégzett munka** a riasztás helyett: besorolás, összegzés, beavatkozás, visszajelzés.
- Havi jelentés** vezetői és technikai szinten, egy dokumentumban.
- Incidens-utókövetés**: mi történt, mi zárta le, mi marad feladatnak.

Nem helyettesíti az IT-csapatot, hanem kiegészíti — az Önök szakembereinek kiterjesztett csapataként működünk. Az antivírus és a tűzfal alapvető, de a mai támadások több lépcsősek, és megkerülik a hagyományos védelmi vonalakat.

¹ IBM, Cost of a Data Breach Report, 2026.

- NIS2-elvárás
- Előfizetési modell
- Végpont- és naplóalapú árazás

BESZÉLJÜNK

Ha most feltörnék a cégét, tudna róla? Nézzük meg együtt.

info@decloudit.com · +36 30 536 4787



OLVASSA BE