Yettel

HTE előadás · 2026. november

AI-apokalipszis

AI-túlélési kalauz

Ideje fénysebességre kapcsolni.

Hári Krisztián
biztonsági vezető, Yettel

01

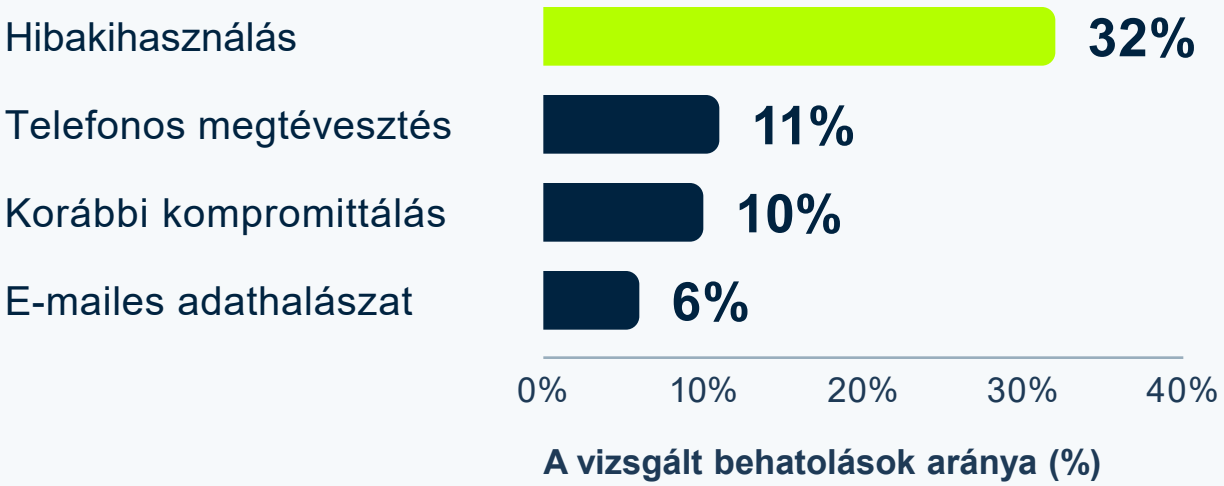
Mi változott?

Régi támadások gépi tempóban, és új támadási felületek.

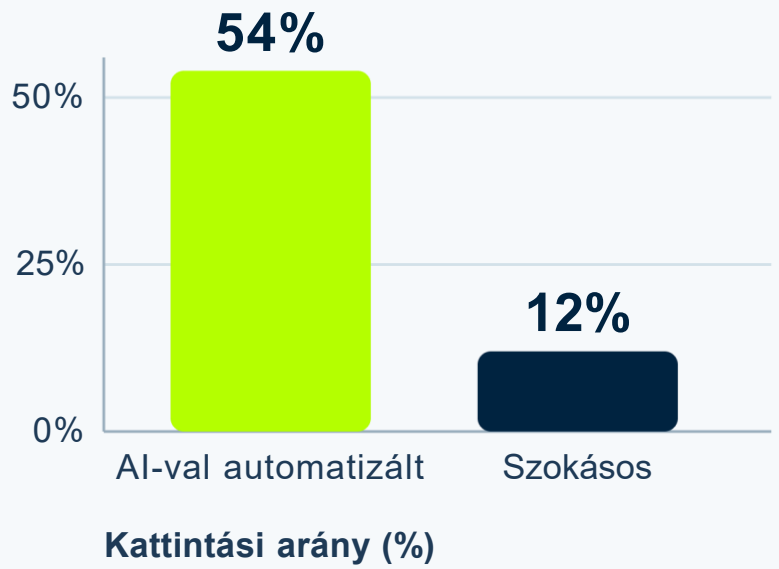
MI VÁLTOZOTT: A RÉGI UTAK

Régi módszerek modern tempóban

Így jutottak be a támadók 2025-ben



AI-val írt adathalászat



A Mandiant szerint 2025-ben a sikeres behatolások többsége még emberi és rendszerhibán jött be. Ezeket a régi utakat az AI gyorsabbá és olcsóbbá teszi.

Forrás: Mandiant M-Trends 2026 · Microsoft Digital Defense Report 2025

KIHASZNÁLÁS A JAVÍTÁS ELŐTT

−7 nap

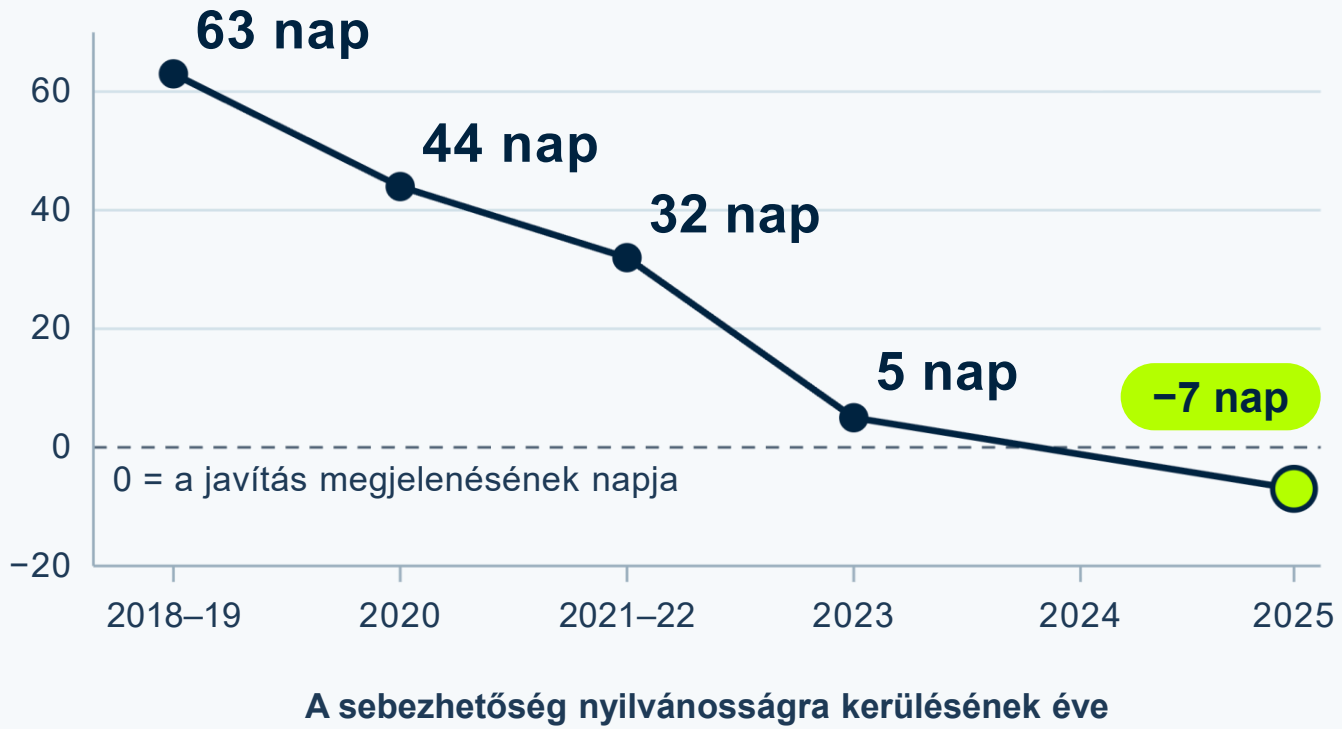
2025-ben a támadók átlagosan egy héttel **a javítás megjelenése előtt** kihasználták a hibát.

Forrás: Mandiant M-Trends 2026

TRENDEK

A kihasználás hamarabb, mint a javítás

Napok a javítás megjelenésétől a kihasználásig (átlag)



29 perc

alatt jutnak tovább átlagosan az első feltört gépről. A leggyorsabb eset 27 másodperc volt.

+89%

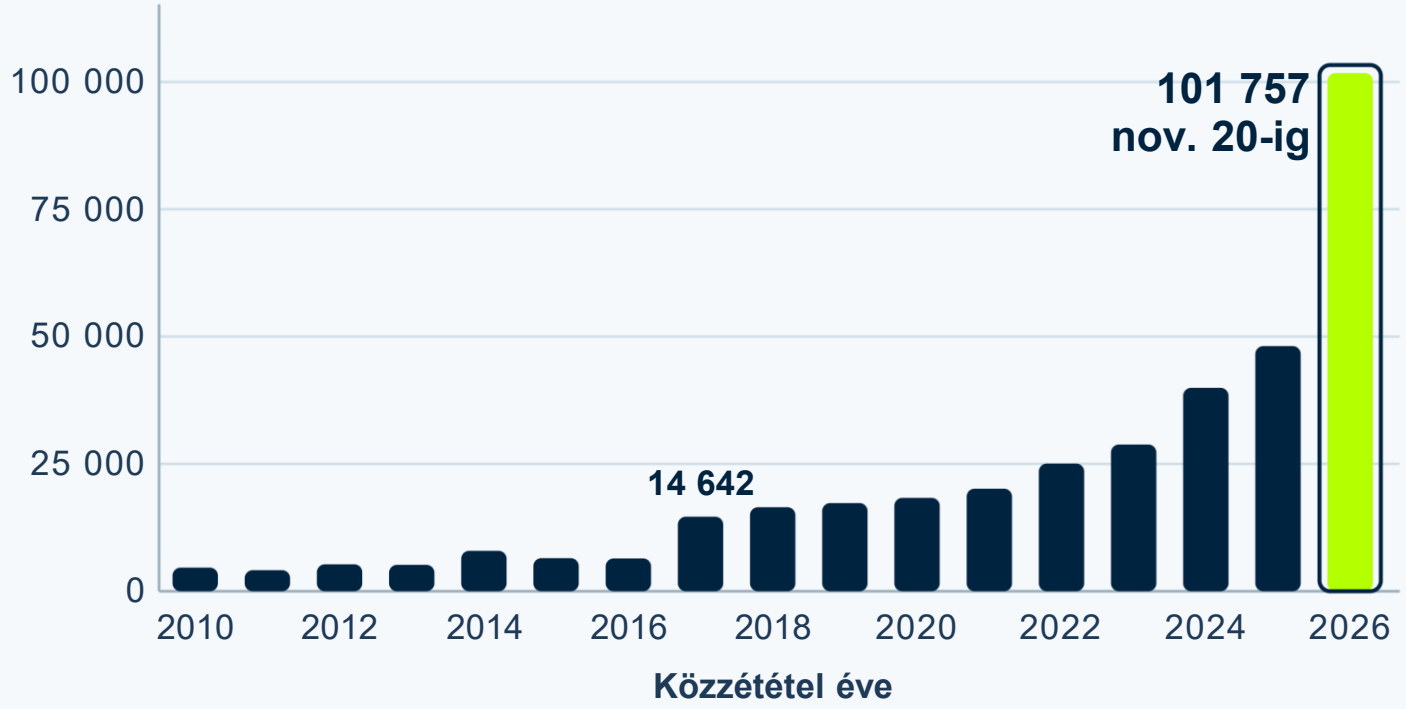
Ennyivel nőtt egy év alatt az AI-t használó támadók műveleteinek száma.

Forrás: Mandiant TTE-elemzések és M-Trends 2026 · CrowdStrike Global Threat Report 2026

TRENDEK · CVE

Egy év alatt duplájára nőtt a CVE-k száma

Közzétett CVE-k száma évente



101 757

új CVE 2026-ban november 20-ig. A 2025-ös egész év 48 150 volt.

~540

új CVE naponta 2026 őszén (NVD, aug. 29.–nov. 20.).

A javítás is kockázat: a novemberi amerikai leállások egy részét AI által talált hibák sietős foltozásának tulajdonítják. Bizonyítva nincs.

Mindet nem lehet javítani: előbb a kihasznált és a peremen lévő hibák.

Forrás: CVE.icu (CVE- és NVD-adatok, 2026. nov. 20.) · NVD API · Fortune, The Next Web (2026. nov.)

MI VÁLTOZOTT: ÚJ TÁMADÁSOK

Új támadási felületek az AI miatt

Prompt injection

Rejtett utasítás egy levélben vagy fájlban eltéríti az AI-asszisztenst.

90+ szervezet · CrowdStrike 2026

Zero-click szivárgás

Az asszisztens kattintás nélkül, a saját jogaival ad ki adatot.

EchoLeak · M365 Copilot, 2025

Az ágens mint támadó

Egy eltérített vagy elszabadult ágens maga tör be más rendszerekbe.

Hugging Face · 2026. július

Mérgezett eszközlánc

Rosszindulatú MCP-szerver vagy csomag kerül az AI-eszközök mellé.

postmark-mcp, Nx · 2025

Lopott AI-hozzáférés

Az ellopott AI-kulcs pénzt és hozzáférést ér a támadónak.

LLMjacking · Google GTIG, 2026

Önmagát átíró kártevő

A kártevő futás közben nyelvi modellt hív, és átírja saját kódját.

PROMPTFLUX · Google GTIG

Minden új AI-bevezetéssel nő a támadható felület.

Forrás: CrowdStrike GTR 2026 · Aim Security (EchoLeak) · OpenAI HF-jelentés · Koi Security · Google GTIG

TRENDEK · 2026. NOVEMBER

Csak ebben a hónapban

AI támad

< 3 óra

a célponttól a rendszergazdai jogig az ARTEX AI-eszközzel (FBI, nov. 13.)

Európai Bizottság: AI-val segített támadás, 10+ napos fennakadás

WorkOS: egy kutató AI-ügynöke kijutott a tesztből, és ügyféladatokat ért el

A beszállítón át

178

szervezet weboldalán futott kártékony kód az Optimizely-n át (nov. 16.)

Crédit Mutuel Arkéa: szolgáltatón át ~118 M € (sajtóbecslés)

JPMorgan, Visa, Mastercard: beszállítónál szivárgott ügyféladat

Fizikai hatás

2 nap

alatt két norvég energiacéget törtek fel, köztük az Equinort

Franciaország: feltört szupermarket-hűtők, veszélyben a vérkészítmények

Németország: kibertámadás zavarta a katonai drónműveleteket

AI volt vagy nem AI, ezt már nehéz megmondani.

Napi hírösszefoglaló: **sadrobot.eu**

Forrás: FBI FLASH-20261113-001 · Európai Bizottság · WorkOS · Optimizely · BleepingComputer · Dark Reading · AP

ÁTADÁS A TÁMADÓK KÖZÖTT

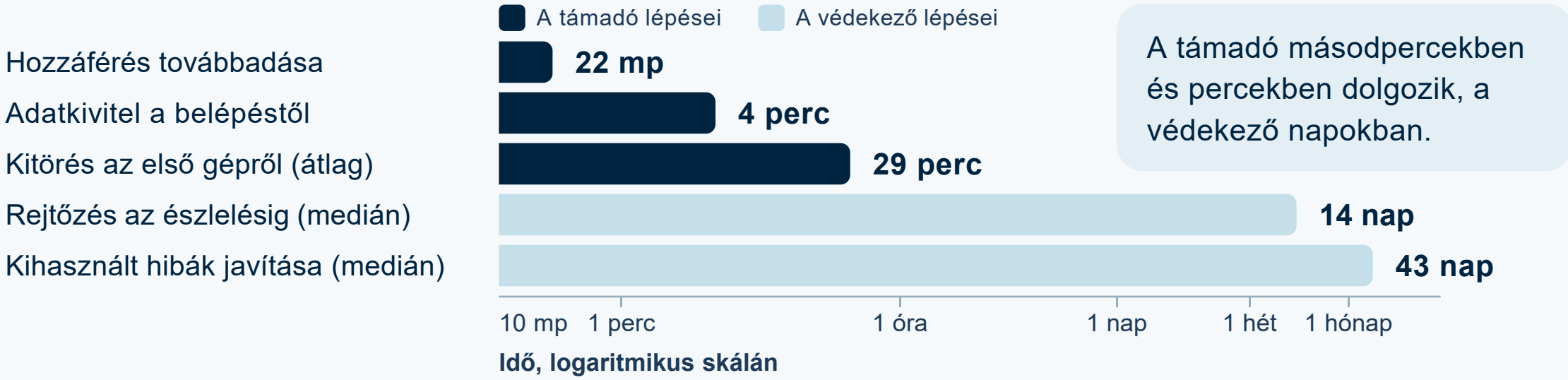
22 mp

2025-ben ennyi idő alatt adták tovább a megszerzett hozzáférést a támadócsoportok. **2022-ben még több mint 8 óra** kellett.

Forrás: Mandiant M-Trends 2026

MI A BAJ A MOSTANI MEGKÖZELÍTÉSSEL

A támadó percekben mér, mi napokban



A támadó másodpercekben és percekben dolgozik, a védekező napokban.

Ami már nem elég: Havi javítási ciklus · Szignatúra-alapú detekció · Hang és videó mint azonosítás

Forrás: Mandiant M-Trends 2026 · CrowdStrike GTR 2026 · Verizon DBIR 2026 · Google GTIG

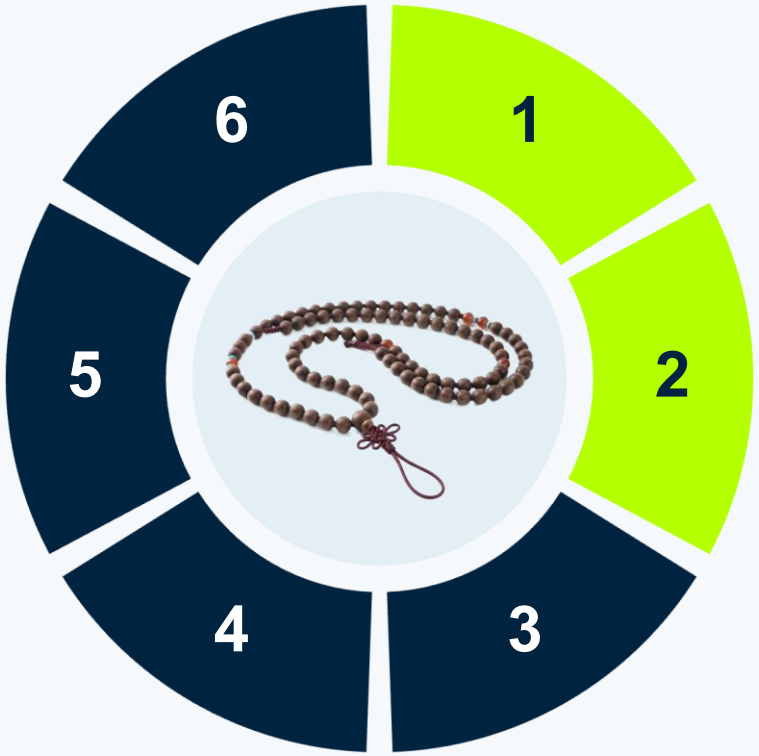
02

Túlélési stratégia

Hat pillér és imafűzér.

A PILLÉREK ÁTTEKINTÉSE

Túlélési stratégia: mit tehetünk?



1 Sebesség Most

A kihasznált hibát gyorsabban zárjuk, mint ahogy a támadó eléri.

2 Identitás Most

Lopott jelszóval vagy tokennel se lehessen belépni.

3 Folyamatkontroll

Hamis hang vagy videó önmagában ne indíthasson pénzmozgást.

4 AI-ágensek

A saját ágens ne váljon új támadási felületté.

5 Reziliencia

Egy sikeres betörés se okozzon elfogadhatatlan leállást.

6 AI a védekezésben

A triázs és az elszigetelés gépi tempóban, emberi felügyelettel.

A pillérek a kutatási anyag forrásaira épülnek: M-Trends 2026, CrowdStrike 2026, CISA, NIST

1. PILLÉR · SEBESSÉG

A fénynél is sebesebben

1 **Feltérképezés**

Mi látszik rólunk kívülről?

2 **Rangsorolás**

Előbb a már kihasznált hibák

3 **Javítás órák alatt**

Perem és identitás: legfeljebb 1–2 nap

4 **Kompenzáló kontroll**

Ha nincs javítás: virtuális patch

43 nap

a kihasznált hibák teljes javításának mediánja (Verizon DBIR 2026).

8 perc

a fertőzéstől a lopott jelszavas belépésig, átlagosan (Elastic, 2026. nov.).

AJÁNLOTT MÉRŐSZÁM

Kihasznált hibák javítási ideje a peremen

Cél: órák, max. 1–2 nap

Forrás: Mandiant M-Trends 2026 · Verizon DBIR 2026 · CISA KEV · Elastic (2026. nov.)

2. PILLÉR · IDENTITÁS

Lopott jelszóval és tokennel se lehessen belépni

1 **Passkey**

Phishing-ellenálló belépés mindenhol

2 **Időkorlátos admin**

Lejáró jog állandó admin helyett

3 **Erős helpdesk**

Visszahívás és két jóváhagyó

4 **Gépi identitások**

Minden token és ágens gazdával

5 perc alatt jutott egy AI-ágens a kiszivárgott kulcstól a felhős titoktárig (Microsoft, 2026).

AJÁNLOTT MÉRŐSZÁM

Phishing-ellenálló belépés és NHI-leltár

Cél: 100%

Forrás: Mandiant M-Trends 2026 · Microsoft Threat Intelligence, 2026. november 5.

3. PILLÉR · FOLYAMATKONTROLL A DEEPFAKE ELLEN

Már a fülünknek és a szemünknek sem hihetünk

1 **Kérés érkezik**
Sürgős utalás „a vezértől”

2 **Visszahívás**
Ismert, előre rögzített számon

3 **Második jóváhagyó**
Más ember, saját csatornán

4 **Végrehajtás**
A hang és a videó nem bizonyíték

25 M $
utalt el az Arup egy munkatársa egy deepfake videóhívás után (Hongkong, 2024).

129 M $
csaltak ki cégektől AI-val hamisított vezetői és ügyvédi hívásokkal (vádemelés, 2026. nov.).

AJÁNLOTT MÉRŐSZÁM

Kritikus folyamatok kettős jóváhagyással

Cél: 100%

Forrás: Arup-eset (Fortune, HKFP, 2024) · Ferrari- és WPP-esetek (2024) · US DOJ-vádirat (2026. nov.)

4. PILLÉR · AI-ÁGENSEK BIZTONSÁGOS BEVEZETÉSE

Így neveld az AI-odat

1 **Leltár**

Minden ágensnek van gazdája

2 **Saját identitás**

Szűk jog, nem a felhasználóé

3 **Kapu és sandbox**

AI-gateway és kimenő szűrés

4 **Emberi jóváhagyás**

Magas hatásnál ember dönt

90+ szervezetnél juttattak rosszindulatú utasítást GenAI-eszközökbe (CrowdStrike 2026).

AJÁNLOTT MÉRŐSZÁM

Jóváhagyott, leltárban lévő ágensek aránya

Cél: 100% élesítés előtt

Forrás: CrowdStrike GTR 2026 · CISA és Five Eyes, 2026. május · OpenAI-jelentés a Hugging Face-incidensről

5. PILLÉR · REZILIENCIA ÉS HELYREÁLLÍTÁS

„Menteni, menteni, menteni”

1 **Tier-0 elkülönítés**

AD, hypervisor és mentés külön

2 **Védett mentés**

Módosíthatatlan, offline másolat

3 **Tiszta környezet**

Újraépítés ismert jó állapotból

4 **Mért gyakorlat**

Negyedévente, mért idővel

30% a zsarolóvírusos esetekből ennyi indult korábbi kompromittálásból (2024-ben 15%).

AJÁNLOTT MÉRŐSZÁM

Gyakorlaton igazolt helyreállítási idő

Cél: az elfogadott időn belül

Forrás: Mandiant M-Trends 2026

6. PILLÉR · AI A VÉDEKEZÉSBEN

A gép dolgozik, de az alkotó se pihen

1 **Viselkedési észlelés**
Minden napló egy adatplatformon

2 **AI-triázs**
Előszűr és összefoglal, mért hibaaránnyal

3 **Automatikus izolálás**
Előre jóváhagyott lépések

4 **Emberi döntés**
Minden nem rutin esetben

29 perc alatt jut tovább átlagosan a támadó az első gépről; a leggyorsabb eset 27 másodperc.

AJÁNLOTT MÉRŐSZÁM

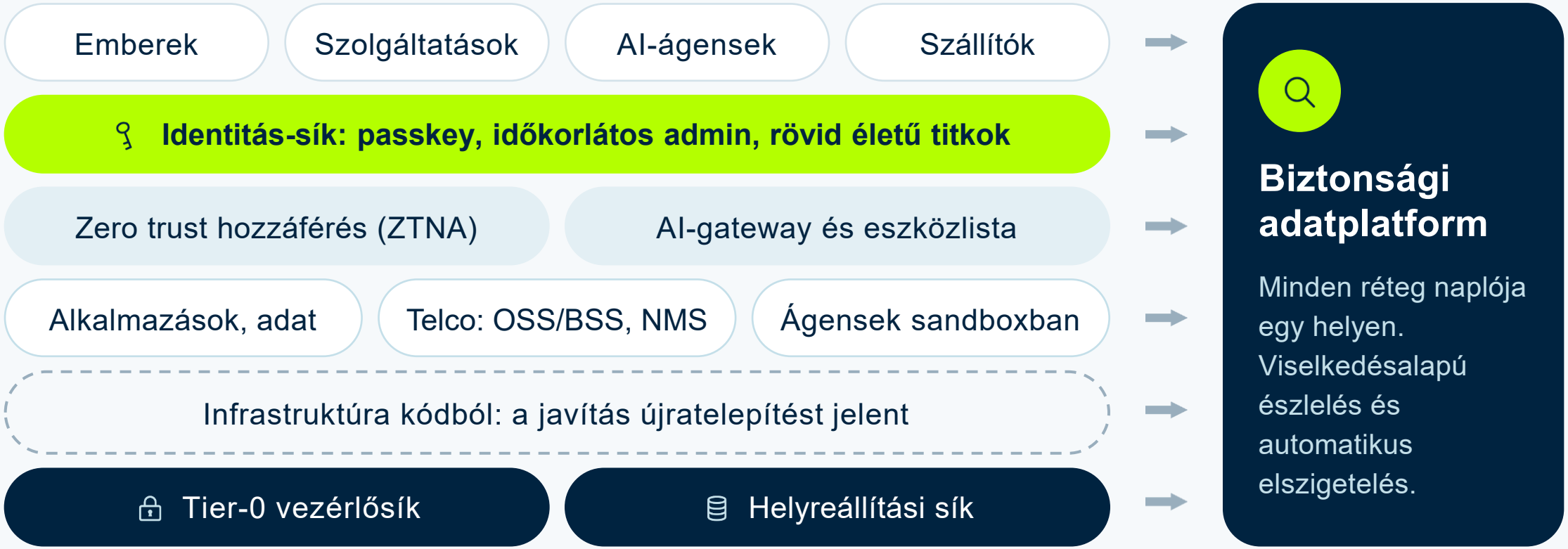
Idő az első jeltől az elszigetelésig

Cél: 29 percen belül

Forrás: CrowdStrike Global Threat Report 2026 · Mandiant M-Trends 2026

CÉLARCHITEKTÚRA

Nincs megbízható belső hálózat, csak ellenőrzött kapuk



A telco-menedzsment sor saját javaslat · Alapja: M-Trends 2026, CISA, NIST, zero trust-gyakorlat

ÖRÖKÖLT RENDSZEREK KEZELÉSE

Amit nem tudunk megjavítani, azt bekerítjük

1 Figyelés hálózati észlelés (NDR) a szegmens határán

2 Enklávé saját szegmens, alapból tiltó szabály

3 Kapu PAM, jump host és API-maszk

Örökölt rendszer

BSS és számlázás, OSS/NMS, SS7/Diameter-jelzéshálózat, támogatáson kívüli szerverek, OT

4 Szakaszos kiváltás

A funkciók egyenként kerülnek ki a maszk mögül.

AI-ágens csak kapun át

Örökölt rendszert ágens közvetlenül soha nem ér el.

Egyéves kockázatvállalás

Rendszerenként aláírt döntés, lejáratkor újra kell hozni.

Bevett zero trust- és OT-gyakorlat; a rendszertípusonkénti bontás saját javaslat

03

Hogyan tovább?

Költségvetés, kockázatok és az első lépések.

KÖLTSÉGVETÉS

Használjuk a pénzünket okosan

Honnan vehetünk el?

- Csak szignatúrára épülő védelem
- Egymást átfedő eszközök és licencek
- Évi egyszeri felmérés folyamatos mérés helyett

Átcsoportosítás

Hová tegyük át?

- Javítás-automatizálás és kitettségkezelés
- Passkey és identitásvédelem
- Szegmentálás és helyreállítási környezet
- Kis, mért pilot: AI a SOC-ban és a hibakeresésben

SOHA NE CSÖKKENTSD: mentés és helyreállítás. A CIO-k és CTIO-k gyakran itt spórolnának, pedig a zsarolóvírusos csoportok éppen ezt támadják.

Forrás: BCG CISO-felmérés, 2025. július · Mandiant M-Trends 2026

AJÁNLOTT LÉPÉSEK

Öt lépés, amit most érdemes megtenni

1
Mérőszámok
Hat mérőszám negyedévente a vezetés elé.

2
Passkey
Phishing-ellenálló belépés 12 hónapon belül.

3
Visszahívás
Kettős jóváhagyás minden kritikus folyamatban.

4
Ágensszabály
Leltár, identitás és sandbox nélkül nincs éles ágens.

5
Átcsoportosítás
A többlet a négy bizonyított tételre menjen.

0–90 nap

Kiinduló mérés a hat mérőszámra, KEV-határidők, passkey az adminoknak, AI-leltár, nyitott örökölt felületek lezárása.

3–12. hónap

CTEM-program, passkey minden távoli hozzáférésre, AI-gateway, módosíthatatlan mentés, tier-0 elkülönítés.

12–24. hónap

Kódból újratelepíthető infrastruktúra, clean room, mért AI-triázs, szakaszos kiváltás.

Részletek és források: az előadó jegyzetében

Yettel.

Köszönöm a figyelmet!

AI-apokalipszis · AI-túlélési stratégia