EY de jó az AI:

NIS2, reziliencia, #sMIszemszájnakingere

Bor Olivér
Manager | Technology Consulting and Cybersecurity

2026
Ernst & Young Consulting Ltd.

The better the question. The better the answer.
The better the world works.

Building a better working world

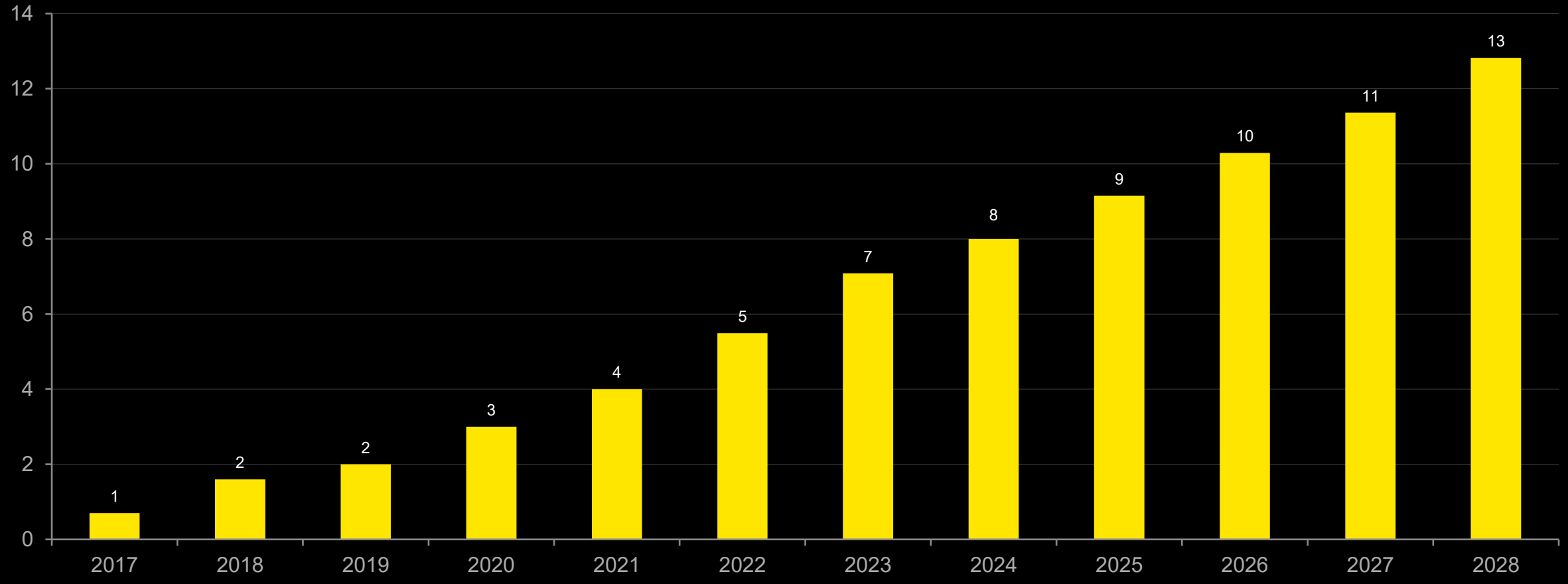
Az örök klasszikus

“Csak két típusú szervezet létezik: az, amelyiket már megtámadtak, és az, amelyik még nem tudja, hogy megtámadták.“

A kiberbiztonság ma már nem csak technológiai kérdés, hanem üzleti kérdés is.

A kiberbűnözés becsült költsége világszerte

(milliárd USA dollárban)



EY

Hogyan fogják megtámadni a szervezetemet a támadók? Az biztos: meg fogják…

Mi a legnépszerűbb támadás?

- A sikeres támadások 85%-a továbbra is az emberi hibára, megtévesztésre épül
- Ezek ellen a legfejlettebb tűzfalak se védenek meg

Miért nem működnek a klasszikus védekezési módszerek?

- Zero-day támadások és APT-k
- Az emberi tényezőt nagyon nehéz kiiktatni
- 7/24 támadói aktivitás
- Cybercrime-as-a-Service (CaaS)

NIS2 – a nagy kép auditori szemüvegen keresztül

Milyen nehézségekkel találkozunk az operatív munka során?

1. **Auditori terheltség:** továbbra is erősen limitált az auditorok száma.
2. **Új érkezők:** sokan nem regisztráltak még, bizonytalanok.
3. **Projektek szállítása:** EY tartja a vállalását, a többi auditorról nincs információnk.
4. **Regisztrált tevékenység:** Sokan csak 1 tevékenységet regisztráltak.
5. **Felkészültség:** a cégek felkészültsége továbbra is nagyon vegyes.

NIS2 - aktualitások számokban

~3 000

érintett szervezet
az SZTFH nyilvántartásában

200+

EY szerződés
felkészítésre és auditra

2026.06.30.

audit határidő
(auditok 20%-a kész)

Jogszabályi alap	2024. évi LXIX. tv. | 7/2024. MK rendelet | 1/2025. SZTFH rendelet
19 kontrollcsalád	Nem adminisztratív kérdések, hanem érettségi szintek — dokumentáció ≠ működő kontroll
Szankciók	Regisztráció elmulasztása: 1–150M HUF | Audit mulasztás: 1–150M HUF | Sorozatos jogsértés: felügyelő kirendelés
Bejelentési köt.	24 óra: bejelentés | 72 óra: incidensjelentés | 30 nap: zárójelentés (NBSZ)

A megfelelés útja: felkészülés nélkül nem megy

1	2	3	4	5
EIR azonosítás és besorolás	**IT biztonsági Keretrendszer**	**GAP Analízis**	**Pre-audit (Próba-audit)**	**NIS2 kiberbiztonsági Audit**
Hatály meghatározása 15 vagy 13-ból akár 3 vagy 4 EIR (arányos megfelelés)	Szervezetre szabott szabályzati keretrendszer és 40+ melléklet (BCP, DRP…)	Hiányosságok azonosítása, kockázatelemzés Alpuló intézkedési terv és javaslatok	Hibák feltárása teszt környezetben, mielőtt az éles audit jön	Független auditorként két lépcsős megközelítés, SZTFH irányába riportálás

EY tapasztalat: A legtöbb szervezet már az elején elakad: nem ismeri a saját rendszereit, nem tudja “milyük van”, nincs IBF, szabályozatlan folyamatok.

AI a kiberbiztonságban: lehetőségek és korlátok

✓ AHOL AZ AI ERŐSEN TÁMOGAT

Fenyegetés-felderítés
Valós idejű anomália-detektálás, SIEM integráció, threat intelligence korreláció.

Log- és eseményelemzés
Nagymennyiségű esemény gyors feldolgozása és mintázat felismerés (tuning szükséges).

Phishing és csalás felismerés
NLP-alapú szűrés, e-mail és deepfake detektálás (kockázatokkal). Beszélni kell a false positive példákról is.

Sérülékenység-kezelés támogatása
Kockázatalapú priorizálás (eszköz- és üzleti kontextus figyelembevételével).

Security awareness támogatása
Személyre szabott oktatási anyagok, interaktív szimulációk generálása.

✗ AHOL AZ AI NEM HELYETTESÍT

GAP elemzés & Audit
Az AI támogathatja az elemzést, de a bizonyíték-alapú validáció és a felelősség emberi, a kontrollok bonyolultsága miatt.

NIS2 megfelelés értékelés
Jogértelmezés, szervezeti kontextus és hatósági megfelelés → emberi döntés szükséges.

Kockázatkezelési döntések
Az AI javaslatokat adhat, de a végső üzleti döntés vezetői felelősség.

Incidenskezelés irányítása
AI támogatja az elemzést és automatizációt, de a kríziskezelés és kommunikáció vezetői feladat.

Etikai & jogi kérdések
AI nem viseli a felelősséget, az auditor igen.

AI a kiberbiztonságban: lehetőségek és korlátok

TECHNIKAI KOCKÁZATOK

Adatmérgezés, prompt injection.

Modell manipuláció.

Detektálás megkerülése.

Új támadási felület.

ELLÁTÁSI LÁNC KOCKÁZATOK

Külső AI modellek és shadow AI.

Nem ismert tanító adatkészlet.

Harmadik fél kitettség.

Beszállítói kontroll szükséges.

GOVERNANCE KOCKÁZATOK

Black-box döntések.

Hiányzó emberi felügyelet.

Nem megfelelő dokumentáltság.

Nem auditálható működés.

MŰKÖDÉSI KOCKÁZATOK

AI függőség.

Fallback hiánya.

AI hibák -> szolgáltatás kiesés.

BC / IR követelmény.

Az AI nem egy Excel makró, hanem egy döntéseket befolyásoló rendszer, ami új kockázatokat hoz be.

AI vs. AI: az új harcmező

TÁMADÓI AI – Mit tud már ma?

Személyre szabott adathalászat

LLM-generált, hibátlan nyelvű, kontextus-tudatos spear phishing — a hagyományos szűrők nem fogják

Automatizált sebezhetőség-keresés

Az AI gyorsan feltérképezi a támadási felületet, amit korábban manuálisan és hosszabb idő alatt végeztek

Adaptív malware

Futás közben módosuló működés, amely képes felismerni és megkerülni a védelmi környezetet

Deepfake alapú manipulácó

Valós idejű hang- és videóklónozás, amely bizalmi alapú támadásokhoz használható

AI-vezérelt lateral movement

Az AI képes a hálózatban navigálni és mintázatok alapján elkerülni az észlelést

VS

VÉDEKEZŐI AI – Hogyan válaszolunk?

AI-alapú anomália-detektálás

A normál működés megtanulása után az eltérések valós idejű felismerése

Automatizált threat hunting

AI proaktívan keresi az ismert és ismeretlen támadási mintákat a loghalmokban 24/7

NLP-alapú phishing szűrés

Az e-mailek tartalmának és kontextusának elemzése, deepfake felismeréssel

AI-vezérelt patch priorizálás

Kockázatalapú sérülékenység-kezelés: melyik CVE-t kell azonnal patchelni a saját környezetben

Szimulált támadások (AI red team)

Folyamatos, automatizált tesztelés a védelem hatékonyságának javítására

EY

Kiberreziliencia három fő pillére

Mikor lesz egy felépített IT biztonsági védelem valóban ellenálló a különféle fenyegetettségekkel szemben?

SZABÁLYZAT

Mihez igazodjon a szervezet biztonsági működése?

MŰKÖDÉS

Hogyan működjön biztonságosan?

AUDIT

Honnan tudom, hogy jól működik?

Mindhárom láb szükséges a biztonságos működéshez, ha egyik hiányzik, a védelem nem biztosított. Ez a NIS2 esetében is igaz!

Kiberreziliencia működtetésének fázisai

1. **Azonosítás (Idetify):**
   Milyen eszközöket kell védenem?

2. Védelem (Protect):
Biztonságos működés kialakítása.

3. Észlelés (Detect):
Mit lát a támadóból a szervezet?

4. Reagálás (Response):
Azonosított fenyegetettségek elhárítása.

5. Helyreállítás (Recover):
Normál működésre való visszaállás.

Köszönöm a figyelmet!

A kibertámadások gyors fejlődése, különösen a mesterséges intelligencia által támogatott támadások, egyre nagyobb kihívást jelentenek a szervezetek és a cégek számára.

Ezért a szervezeti kiberreziliencia fenntartása érdekében, a jogszabályoknak való megfelelés mellett kulcsfontosságúvá válik az ilyen típusú fenyegetések időben történő felismerése és a hatékony felkészülés.

Bor Olivér

Manager | Technology Consulting and Cybersecurity

Ernst & Young Tanácsadó Kft.