



**ALVERAD**  
CYBERSECURITY

By **SGS**

# NIS 2

**Kiberbiztonsági auditokon az IT és OT  
rendszerek, mint EIR-ek**

2026. 04. 20.



# 2024. évi LXIX. törvény

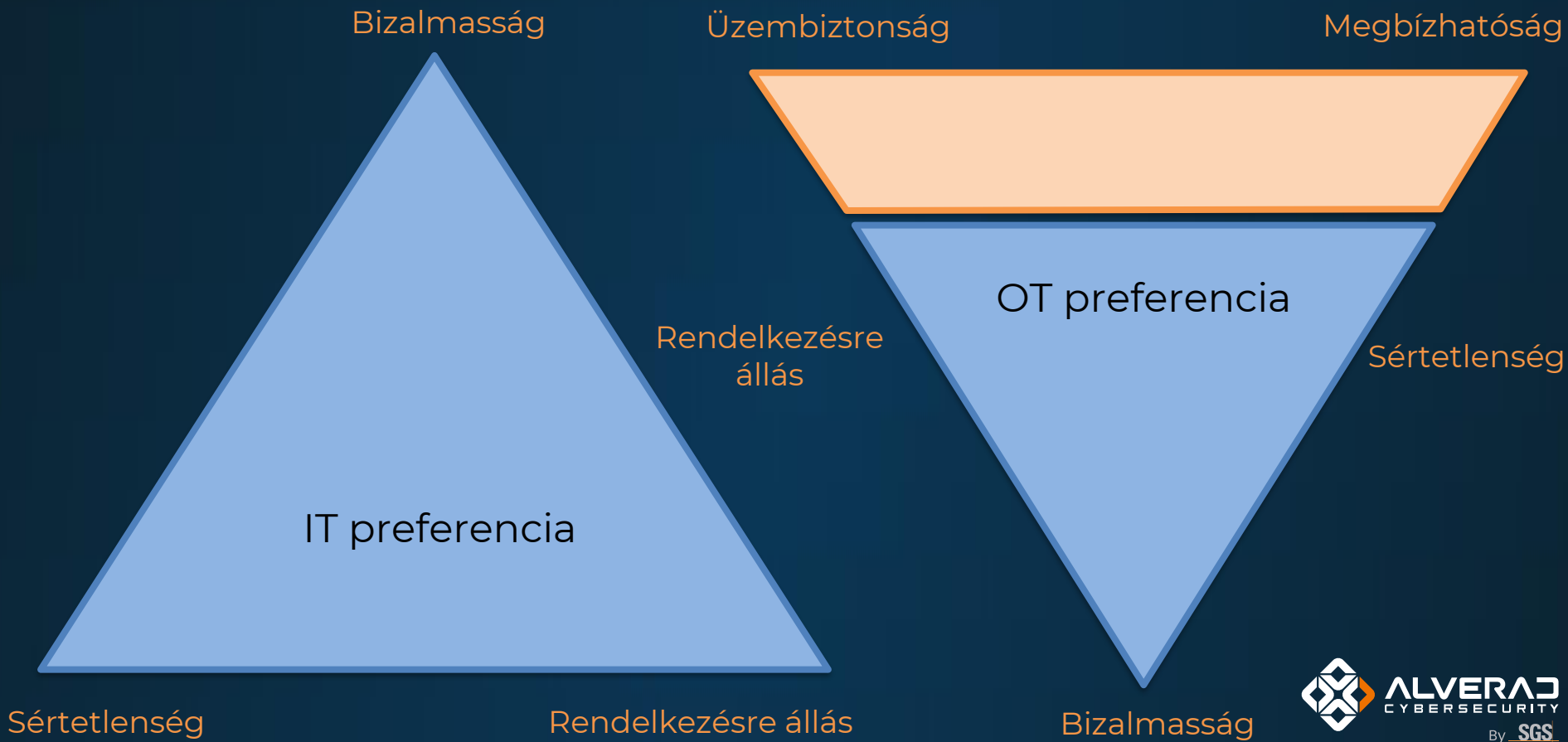
## Magyarország kiberbiztonságáról

4.§

24. elektronikus információs rendszer:

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, **ideértve a kiber-fizikai rendszereket**

# IT ≠ OT



## Information Technology (IT)

## Operational Technology (OT)

### Összetevők, komponensek

Szerverek, munkaállomások, adattárak, felhő, biztonsági eszközök, mobilkészülékek, webalkalmazások, hálózati eszközök.

PLC/DCS, SCADA, adatgyűjtők, szenzorok, motorok és egyéb terepi eszközök, protokollkonverterek, gyártásirányítók.

### Életciklus

3-5 éves életciklus

10-25-50 éves életciklus

### Működés

Együttműködő, összekapcsolt alkalmazások, rendszerek és hálózatok összessége.

Szigetrendszerű, önálló működés.

### Biztonsági koncepció

„Data first”, adatközpontú szemlélet.

„Process first”, folyamat központú szemlélet.

### Személyzet

Rendszergazdák, IT mérnökök, biztonsági mérnökök és felhasználók. „Fehérgalléros” munkavállalók.

Operátorok, karbantartók, terepi mérnökök és automatizálási mérnökök. „Fehér- és kékgalléros” munkavállalók.

### Üzemeltetés

Az IT rendszereket a szervezetek maguk üzemeltetik és tartják karban, illetve igénybe vehetnek alvállalkozó (outsourcer) partnert.

Az OT rendszereket jellemzően a szállítók, integrátorok vagy a gyártók üzemeltetik és tartják karban.

### Elhelyezkedés

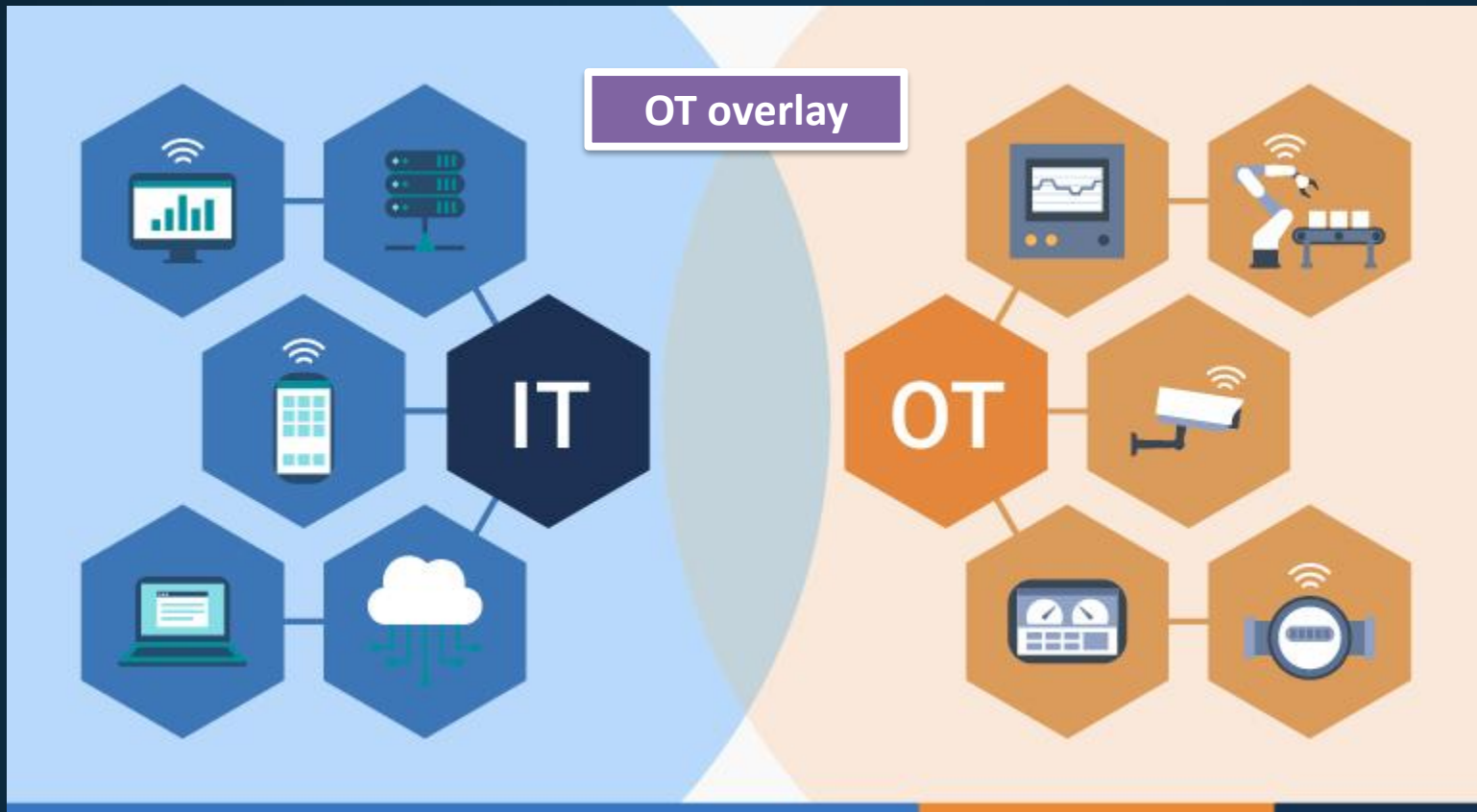
Centralizált rendszerek, adatközpontokban, szerverszobákban.

Decentralizált és akár elszigetelt működés, nagy távolságok, és terepi viszonyok.

# IT ≠ OT - egységes értékelés

IT: NIST 800-53

OT: NIST 800-82



# Tipikus problémák és válaszlépések

- › **EIR / IT – OT – kevés vagy sok.** Az audit fókusza kérdése az EIR helyes lehatárolása, tartalmának megállapítása.
- › **IT és OT kockázatok** – hatáselemzés, de mi ellen véd?
- › **Dobozos megfelelétlenség** – még IT-re se lenne elég, utána meg copy-paste (VHS)
- › **OT dokumentáltság** – minden van, „csak: ...”.
- › **IT – OT elválasztás** – elmélet: minden hermetikusan le van választva, valóság:
- › **Távoli elérés** – csak az üzemeltető, csak amikor és ahogy akarja (jelszó?)
- › **Térkép és táj** – szabályozott „valóság”
- › Az OT-ban „semmilyen kontrollt nem lehet” bevezetni (NIST 800-82, IEC 62443)
- › Vizibilitás – Kontroll – Reziliencia hiányára vezethető vissza.

# 10-15 év

## Kerülő megoldások



- Architektúrák
- Komponensek képességei
- Szemléletmód
- Fehér és kék galléros párbeszéd
- Legacy rendszerek
- Életciklus vs EoL (tervek szerint vagy sem)
- Korlátozott javíthatóság
- Beszállítói függés (IT – OT)

## Beépített biztonság



# Köszönöm a figyelmet!

- Angyal Adrián
- [angyal.adrian@alverad.hu](mailto:angyal.adrian@alverad.hu)