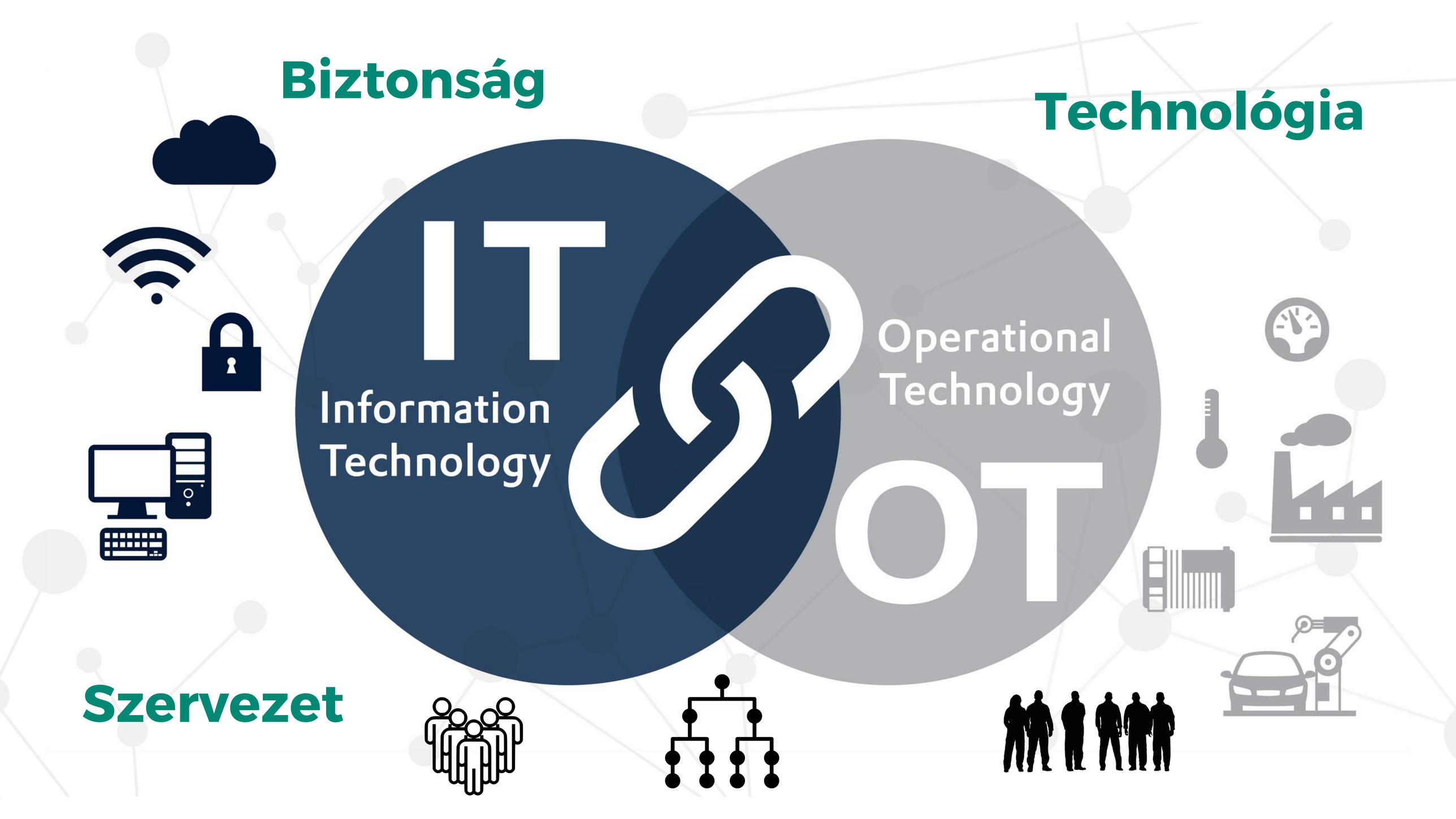
“Persze, hogy tudtam… csak nem sejtettem”

IT-OT integráció a NIS2 idején

Bóna Péter, CEO, Owner

COM-FORTH
IPARI INFORMATIKA

2025. március 19.


Biztonság
Technológia
IT
Information Technology
Operational Technology
OT
Szervezet

IT-OT INTEGRÁCIÓS KIHÍVÁSOK

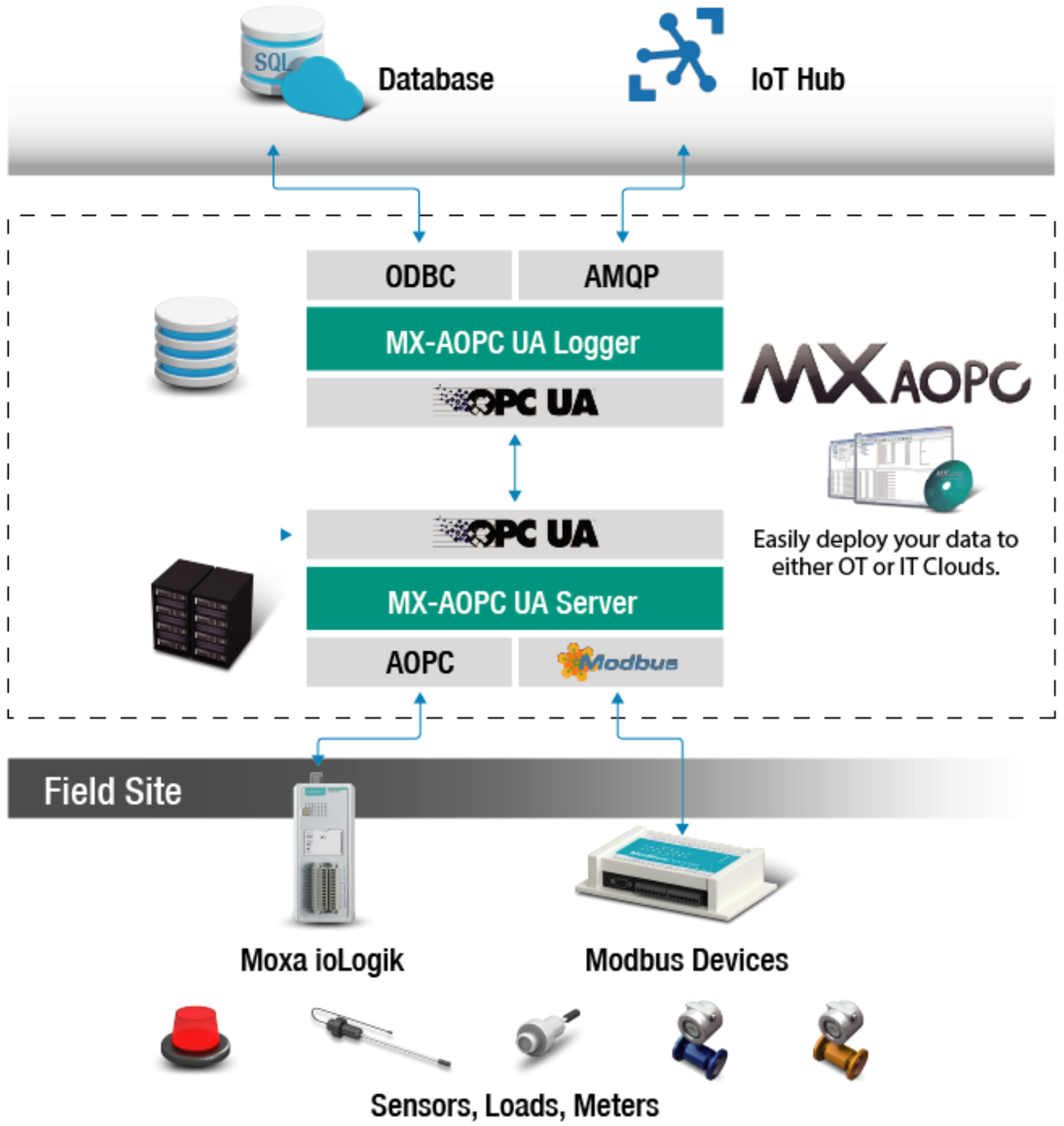
OT protokollok integrálása IT környezetbe
(Modbus TCP, Ethernet/IP, PROFINET…)
- interoperabilitás

Biztonsági aspektusok
- átjárhatóság, szegmentálás

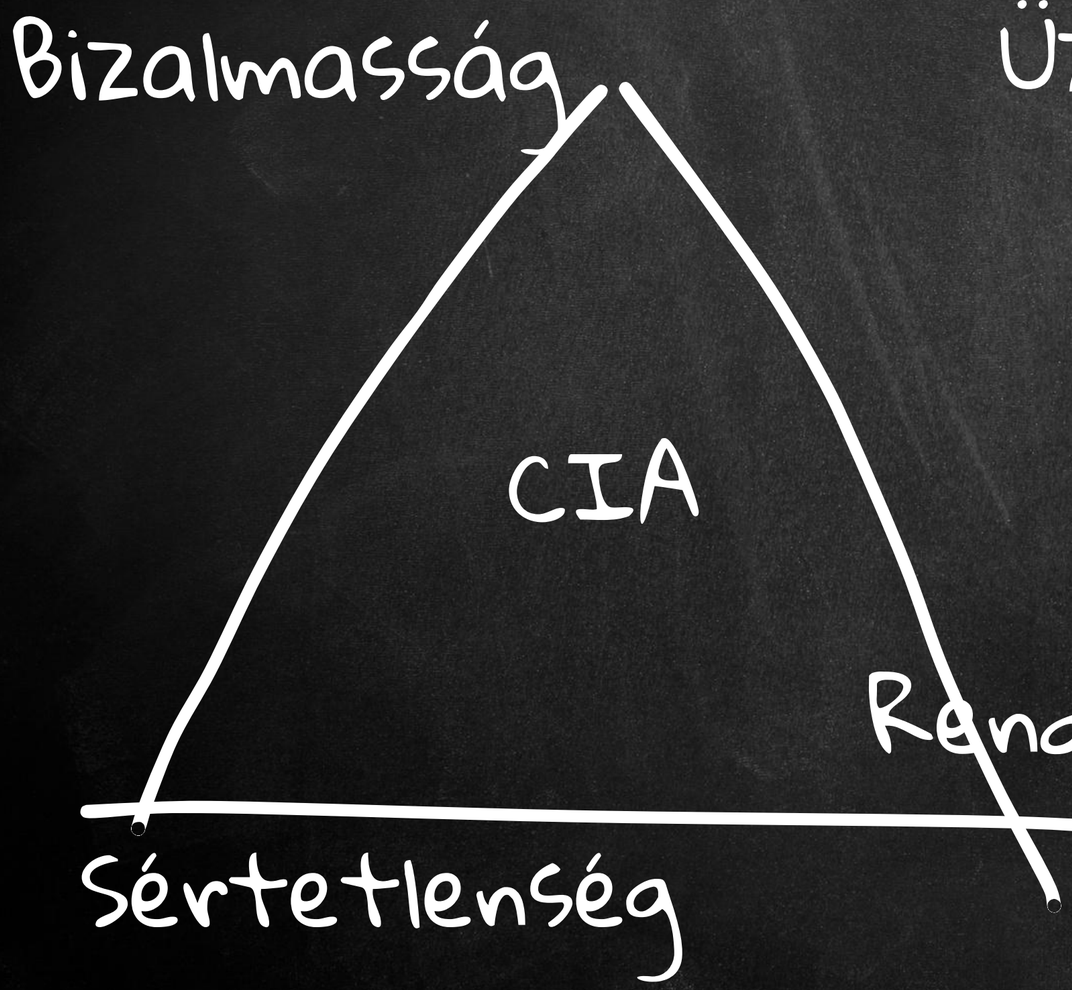
Windows XP/7 gépek hálózatba kötése

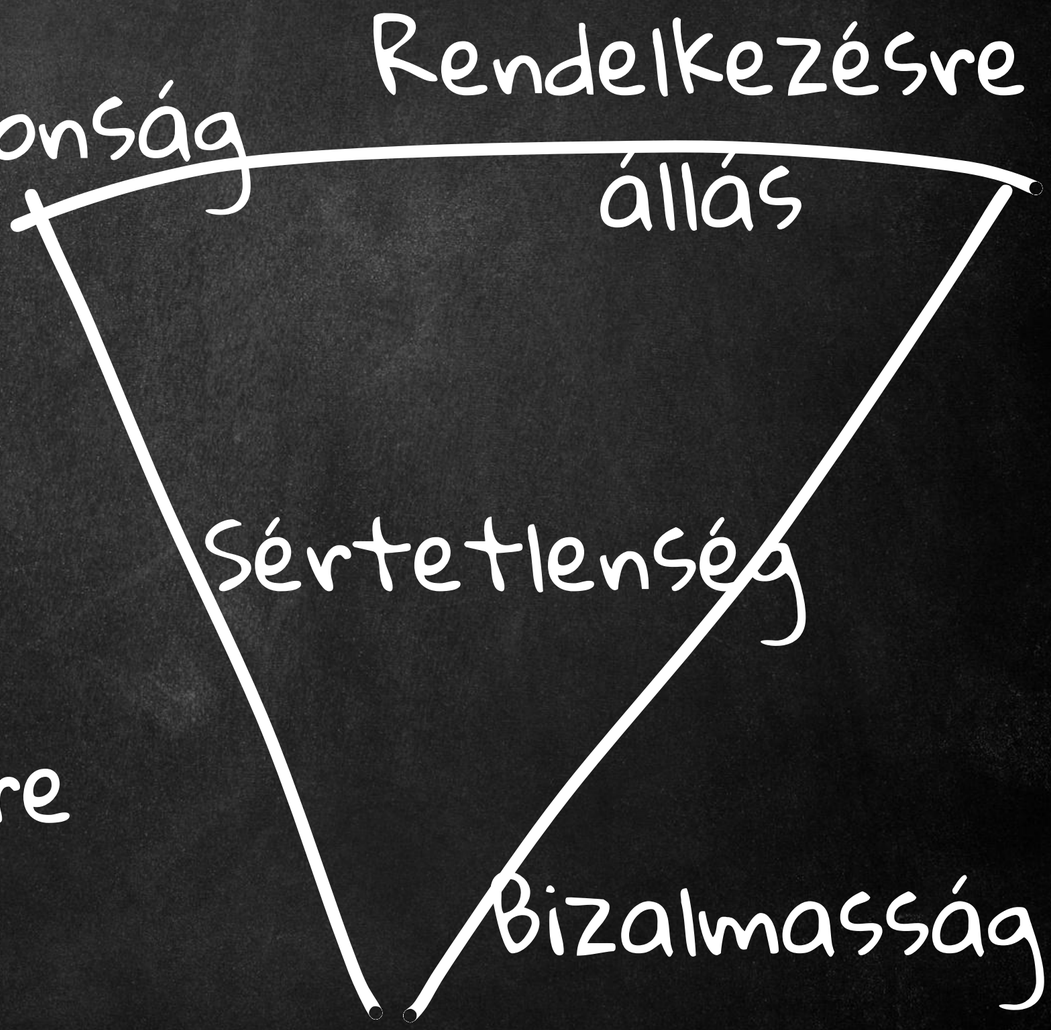
Biztonságos távoli elérés kialakítása

Szervezeti kihívások
IT-OT csapat létrehozása, különböző szakemberek együttműködése, eltérő preferenciák kezelése)



IT ≠ OT


Bizalmasság
CIA
Rendelkezésre
állás
Sértetlenség


Üzembiztonság
Rendelkezésre
állás
Sértetlenség
Bizalmasság

Egy gyártó vállalat számára a legfontosabb, hogy menjen az üzem...

TERMELNI BÁRMI ÁRON

Az ipar 4.0, az adatgyűjtés, az optimalizálás és a kiberbiztonság is másodlagos

IT ≈ OT

- Végpontvédelem telepítése
- Frissítések és security patch-ek telepítése
- Eszközök zárolásának kérdése
- Behatolásvizsgálat (pen test)
- IPS vs IDS hatása a gyártásra

...

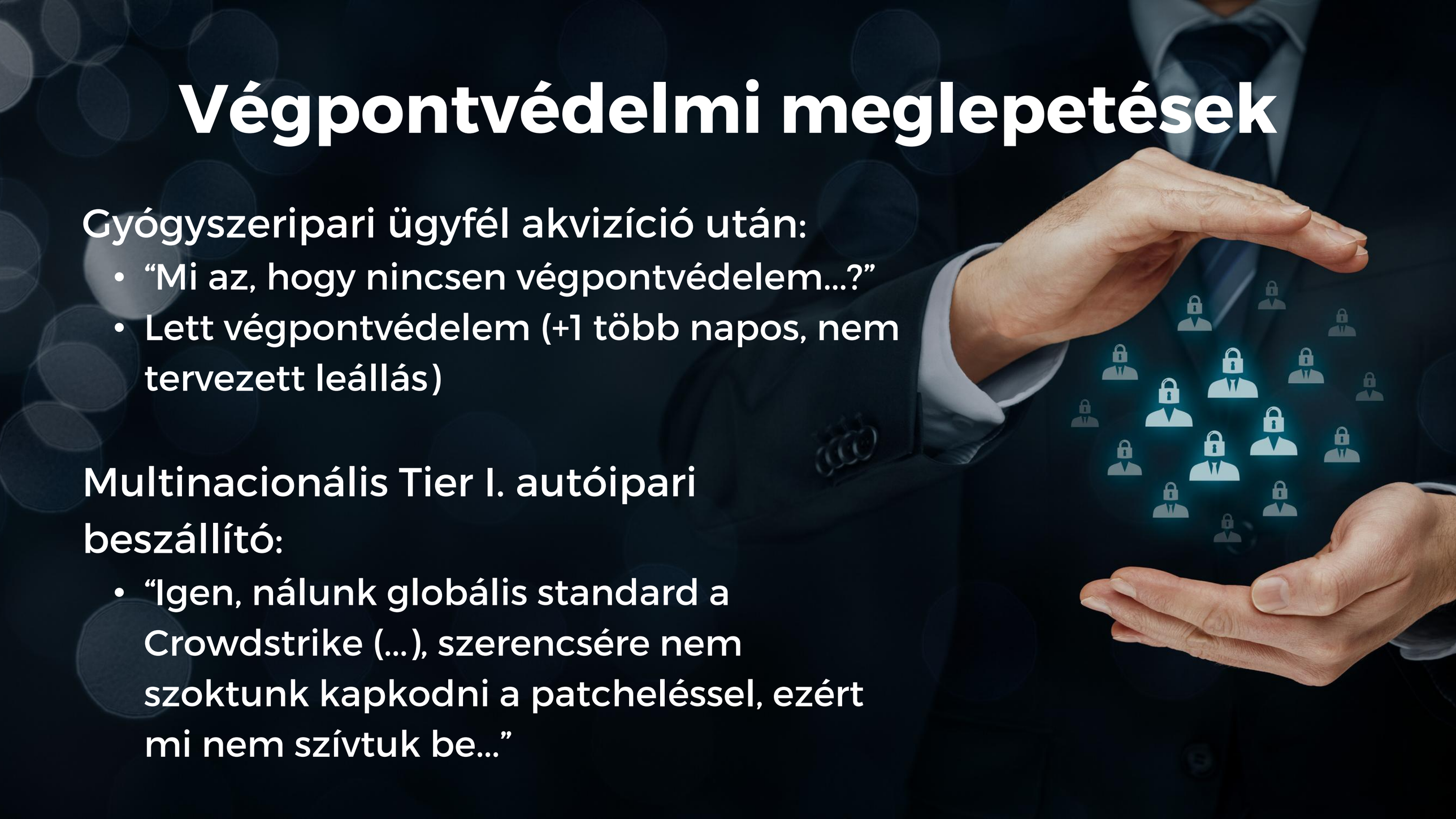
Végpontvédelmi meglepetések

Gyógyszeripari ügyfél akvizíció után:

- “Mi az, hogy nincsen végpontvédelem…?”
- Lett végpontvédelem (+1 több napos, nem tervezett leállás)

Multinacionális Tier I. autóipari beszállító:

- “Igen, nálunk globális standard a Crowdstrike (…), szerencsére nem szoktunk kapkodni a patcheléssel, ezért mi nem szívtuk be…”



Miért nem elég egy IT tűzfal?

Mérnökünk az üzemben:

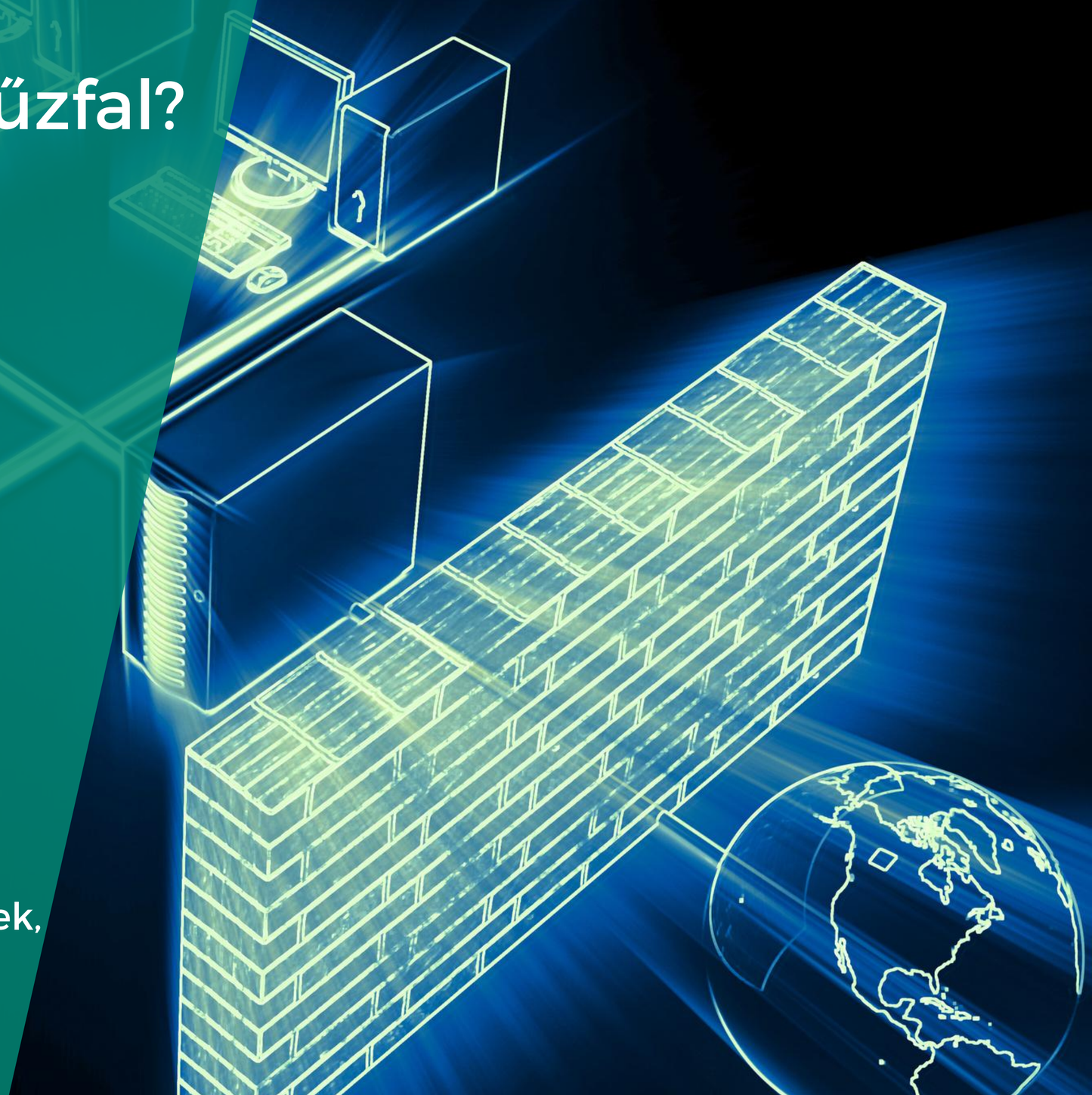
- “Hova dughatom be a gépem?”
  “Bárhova…”

Szakmai esemény élő demó:

- “Igen, és itt a kolléga távolról pontosan látja, hogy mi történik, a pillanatnyi adatokat, OEE stb., de nem tudja elindítani / leállítani a gyártást.”
- Mérnök kolléga halkan megjegyezte:
  “hát, az a baj, hogy de…”

Autóipari Tier I. beszállító rendszerintegrátora:

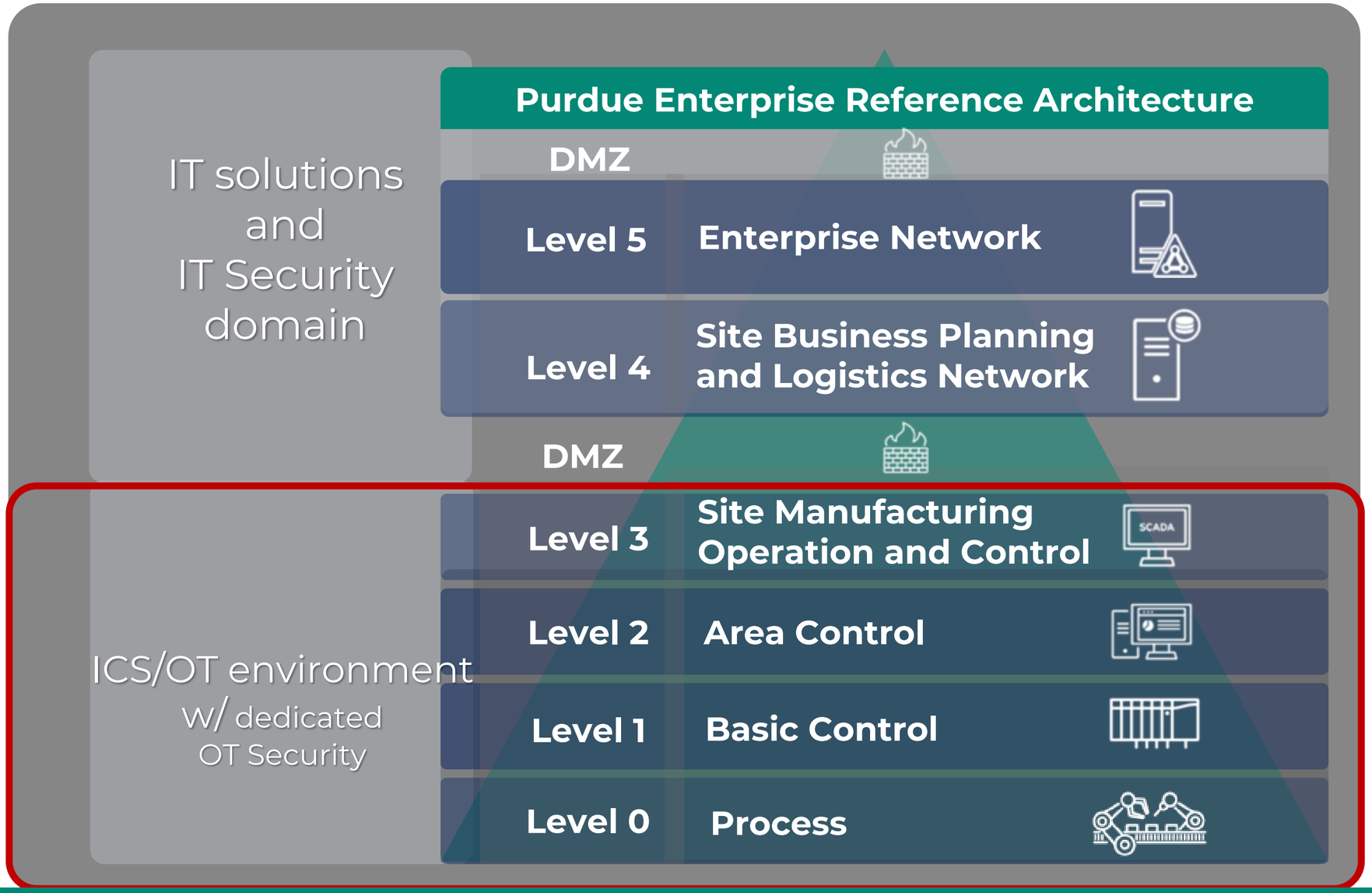
- “Bent az üzemben, bármihez hozzáférek, bármit tönkre tudnék tenni (…) Nesze Neked NIS2”



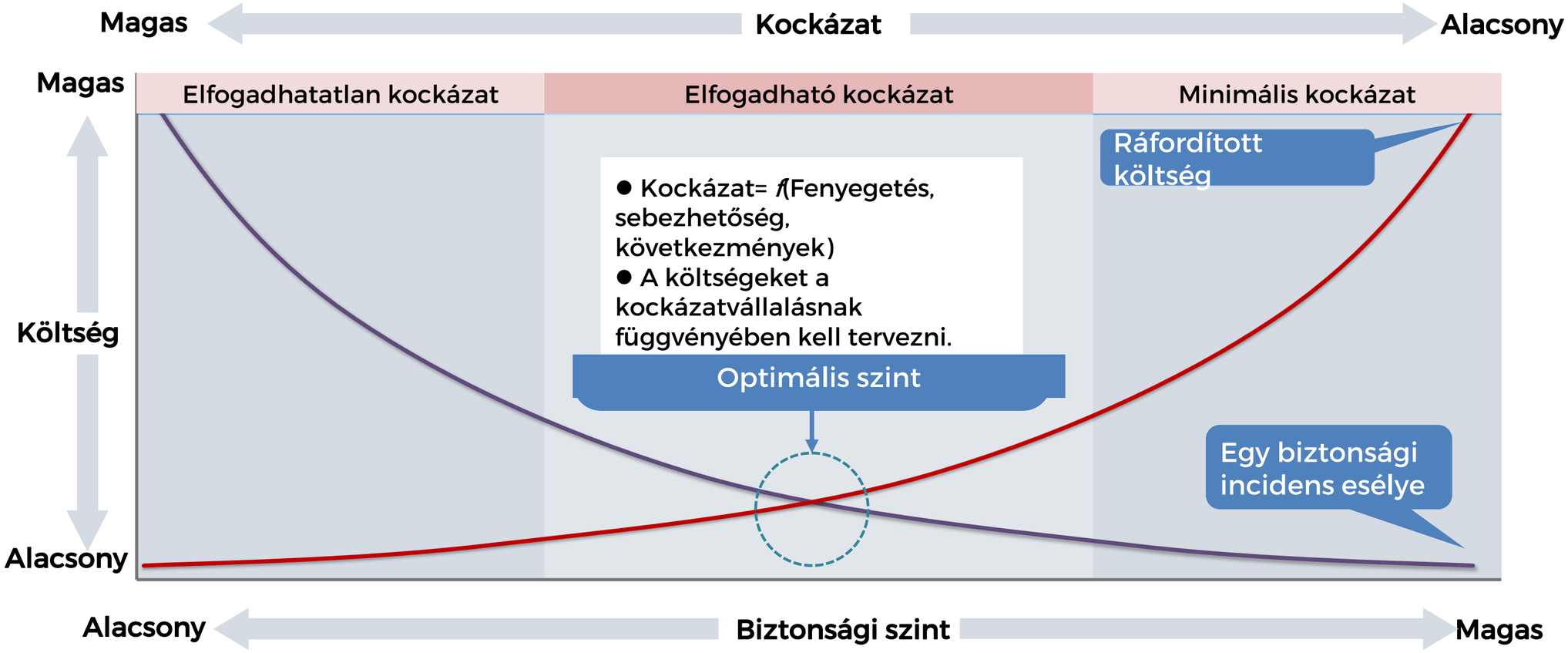
IT ⟷ OT

- Eltérő típusú emberek
- Eltérő gondolkodásmóddal és nyelvezettel
- Korlátozott rálátással egymás területére
- Eltérő KPI-okkal, kockázatokkal
- Szervezetileg általában az IT alá rendelve, ha kiberbiztonságról van szó...

IT-OT biztonság a Purdue modell alapján



IT-OT kockázatelemzés



OT hálózati eszközök elvárt funkciói a „NIS2 megfelelésért”

Tűzfal Switch Mindkettő Felügyeleti szoftver

Hálózat és hálózati eszközök

- (Mikro)szegmentáció
- Zónakontroll és zónavédelem
- Redundancia
- Hálózatvédelem
- Protokollvédelem
- Sérülékenységek kezelése
- Javítások
- Felügyelet, monitoring
- Hálózatmonitoring támogatás
- SNMP v2, v3 (v1 nem javasolt)
- Syslog (SIEM/SOC integráció)
- QOS
- Port-anomáliák, torlódás, csomagvesztés
- Hurkok észlelése
- Protokoll monitoring, alkalmazás riportok, stb.

- Ellenálló képesség (környezeti)
- Menedzselhető eszközök
- VLAN szeparáció
- Port mirroring N:1
- Naplózási képesség
- Hitelesítés, jogosultsági szerepkörök, stb.

Karbantartási ablak

- A javítások telepítése forgalomkiesést okoz(hat)
- Redundáns eszközök esetében eszközről-eszközre
- Javítások minősége – visszaállíthatóság
- Centralizált menedzsment
- Konfigurációmentés (centralizált, automatikus)
- Konfiguráció visszatöltése (centralizált, manuális)

- Forgalomszabályozás
- Hálózati hozzáférés-védelem
- Behatolásvédelem
- Hálózati kártékony kód-elleni védelem
- Protokollvédelem, DPI
- Tartalomszűrés, stb.

OT hálózatvédelem

- Protokollelemzés, anomáliaészlelés
- Változók, értékek és paraméterek figyelése (pl. MODBUS)
- Behatolásészlelés (IDS)
- Behatolásvédelem (IPS)
- Asset Inventory a hálózati forgalomból (dinamikus)

NIS2 és az ipari hálózatok…

Milyen ipari hálózati eszközt válasszak, hogy megfeleljek a NIS2-nek?

- Nincs olyan, hogy egy eszköz NIS2 megfelelőséggel rendelkezik!
- Legfeljebb marketing szempontból.
- A NIS2-t minden tagállam saját módszer alapján implementálja.

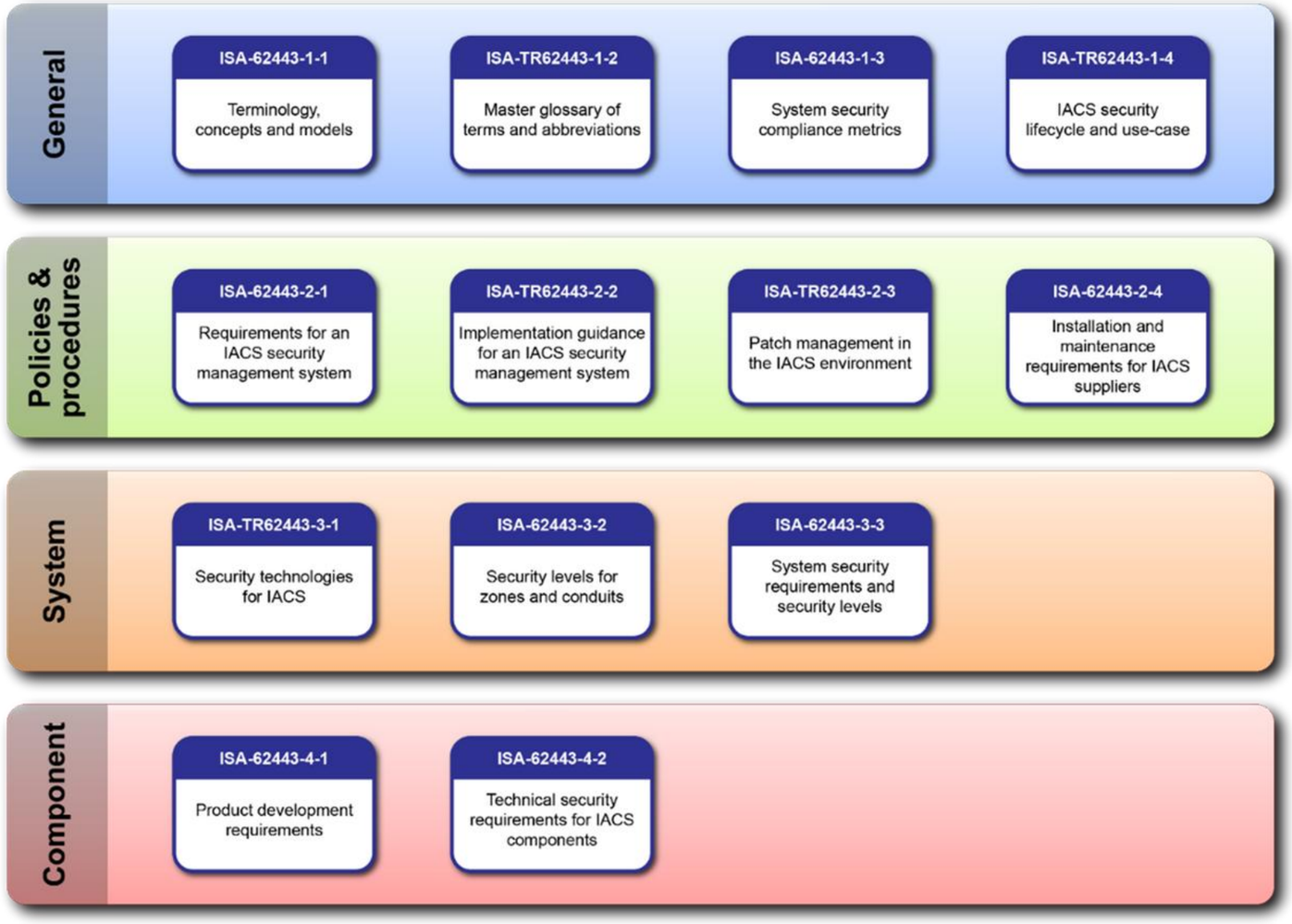
MOXA

Overview Applications Product Portfolio Contact Us

	EDS-4008 Series	EDS-4009 Series	EDS-4012 Series	EDS-4014 Series	EDS-G4008 Series
					
Supports PoE	✓	-	✓	-	-
10/100 FE	Up to 8 ports	9 ports	8 ports	8 ports	-
GbE	Up to 4 ports	-	4 ports	4 ports	8 ports
2.5GbE	-	-	-	2 ports	-
90 W PoE Ports	Up to 4 ports	-	Up to 8 ports	-	-
NIS2 KOMPILANT	OFKORSZ All modells are kompilant!				
Power Input	Low-voltage models: 12/24/48 VDC High-voltage models: 110/220 VDC/VAC				

Az IEC 62443 tanúsítás viszont már előny
Az IEC 62443 az ipari kiberbiztonság szabványa

IEC 62443-4-2 tanúsítvánnyal rendelkező OT hálózati eszközök



ISA-62443-4-1

Product development requirements

IEC 62443-4-1

A Moxa megkapta az IEC 62443-4-1 tanúsítványt, melyet a LCIE Bureau Veritas állított ki. Az EDS-(G)4000 és RKS-G4000 sorozat fejlesztése a teljes termékfejlesztési életciklus során az IEC 62443-4-1 szabványt követi.

ISA-62443-4-2

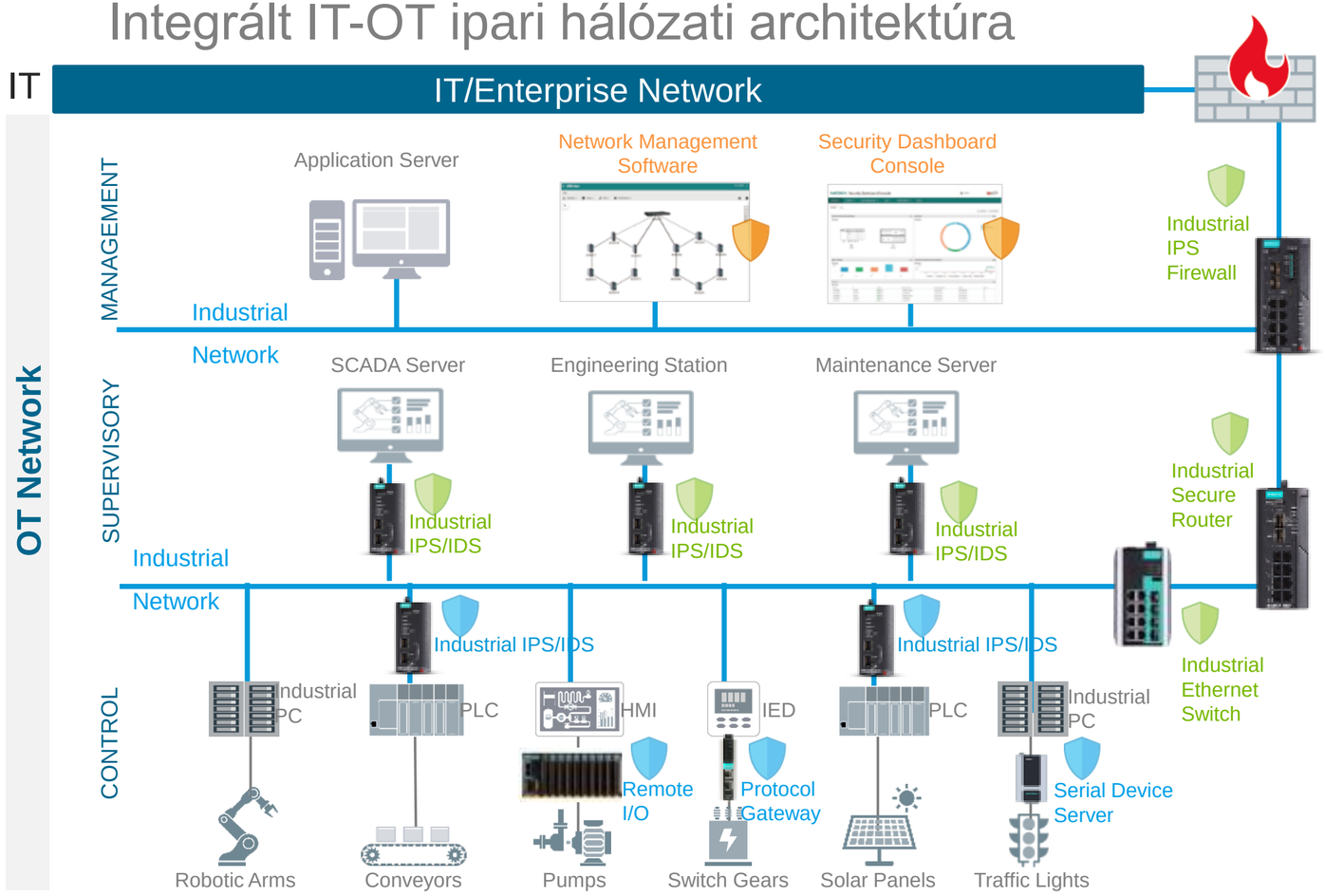
Technical security requirements for IACS components

IEC 62443-4-2

EDS-(G)4000 és az RKS-G4000 terméksorozatok megfelelnek az IEC 62443-4-2 által megfogalmazott biztonsági követelményeknek, és megkapták a tanúsítványt az LCIE Bureau Veritas szervezettől.

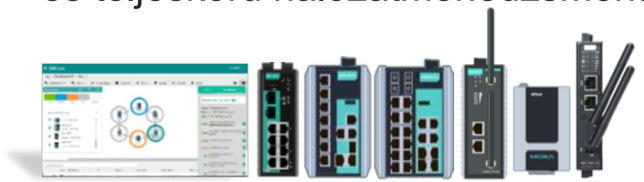
Biztonságos OT hálózat- és végpontvédelem

Integrált IT-OT ipari hálózati architektúra



Biztonságos hálózati infrastruktúra

Rétegelt védelem IEC 62443-4-2 tanúsítvánnyal rendelkező eszközökkel és teljeskörű hálózatmenedzsmenttel.



Natív OT kiberbiztonsági megoldások

Behatolásvédelmi és –detektálási rendszerek (IPS/IDS), natív OT végpontvédelem, virtuális patch-elés.

KÖSZÖNÖM A FIGYELMET!

Bóna Péter

CEO, tulajdonos

MOBIL: +36-30-2007239

EMAIL: pbona@comforth.hu

WEBOLDAL: www.comforth.hu

COM-FORTH
IPARI INFORMATIKA