kontron

Explore the Kontron Group

We are a fast-moving multinational technology leader.

Biztonságban vannak a gyártógépei? Az OT security aktualitásai

Piszker György MBA, CISSP
Kontron Hungary
Rendszer Architect vezető

OT/ICS Security

- Operational Technology vagy Industrial Control Subsystem
  - Az ipari vagy gyártási folyamatok vezérlésére használt elektronikus, vagy digitális rendszerek
    - PLC-k, SCADA rendszerek, gyártói felügyeleti rendszerek, stb.

IT és OT/ICS Security

Prioritások

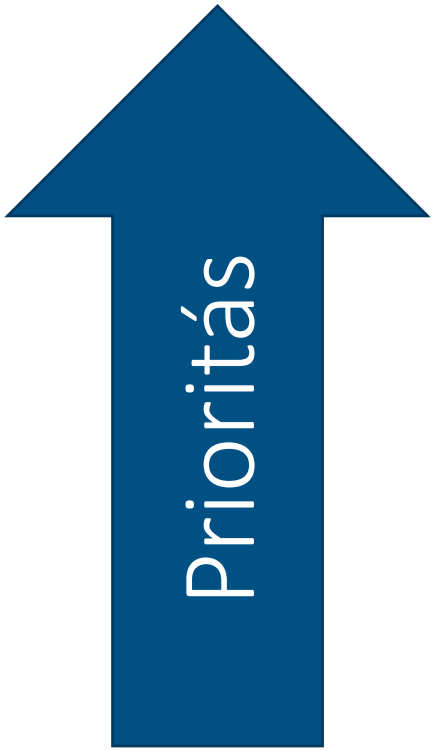
Security célok

IT rendszerek

Confidentiality – Bizalmasság

Integrity - Egységesség

Availability - Elérhetőség



OT/ICS rendszerek

Operability - Működőképesség

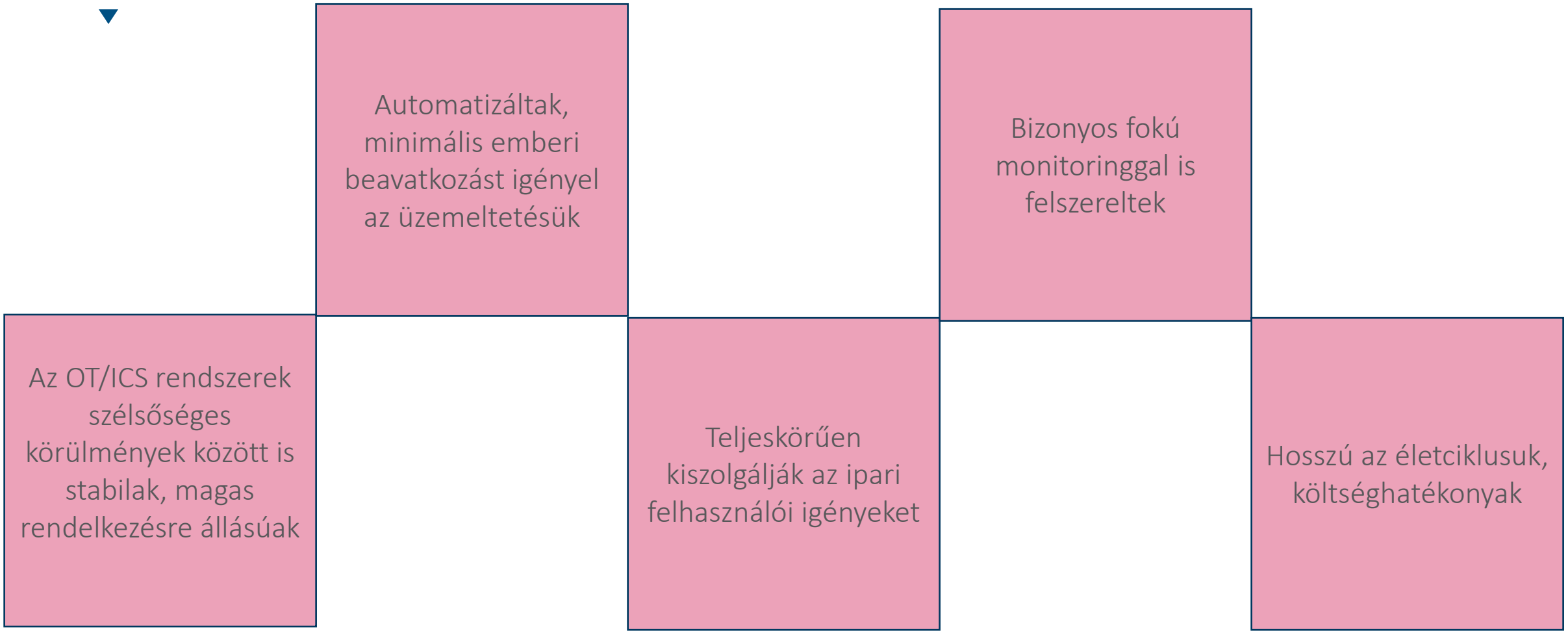
Availability - Elérhetőség

Integrity - Egységesség

Confidentiality – Bizalmasság

OT/ICS Security

Iparági tapasztalatok - Pro



Tulajdonképpen minden rendben van.

OT/ICS Security

Gyakori - Iparági tapasztalatok - Kontra

hálózati szeparáció nélkül integráltak az IT hálózattal

A végpontok száma nem pontosan ismert, esetleg van manuális asset menedzsment

A végpontok forgalmai nem ismertek, nem monitorozottak és nem felügyeltek

A rendszerek software frissítése az éves tervezett karbantartáskor kerül elvégzésre

A felhasználók több esetben közös felhasználónevet és jelszót használnak

A menedzsment és monitoring rendszereik nem támogatott OS-en (WinXP; Win7) futnak

Az access control nem megoldott, gyakran előfordul Internetre kötött Remote Desktop elérés is

A rendszerek OS, alkalmazás, adatbázis mentései nem megoldottak

Az OT/ICS rendszerekre nem léteznek frissen tartott, ellenőrzött, begyakorolt DRP tervek

Adatvédelmi incidens átlagos észlelési ideje 2022-ben:

277 nap

Ellopott vagy feltört hitelesítési adatok átlagos észlelési ideje 2022-ben:

327 nap

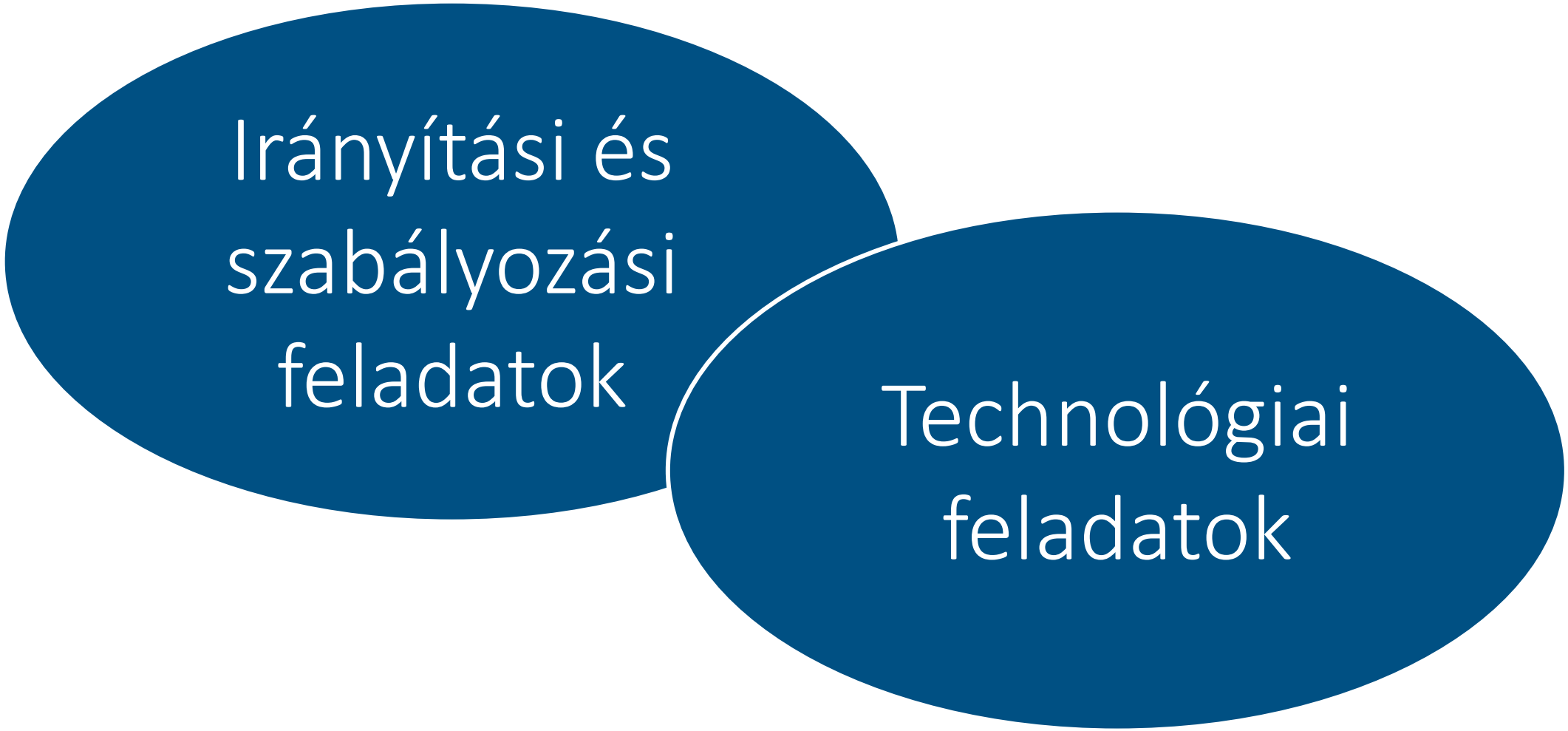
Mélyebbre tekintve, van tér a fejlődésre

OT/ICS Security

Megtörtént esetek

Iparág	Szervezet	Támadási típus	Jelenség és hatás	Költség
Energia/hadiipar	iráni atomprogram	Stuxnet	Termelő eszközök fizikai tönkretétele, program visszavetése évekkel	ismeretlen
Energia	Ukrenergo Villamos energiaszolgáltató	OT specifikus malware (Crashoverride, Blackenergy)	Kijev áramellátásának részleges kiesése	225.000 fogyasztó áramellátás nélkül
Fémipar	Norsk Hydro	Ransomware	Az automatizált gyártói rendszerek kiesése	70M USD
Szállítmányozás	Fedex	Ransomware, NotPetya	IT üzemeltetési kiesés, szállítási és értékesítési kieséssel	300M USD
Olajipar	Colonial Pipeline	Ransomware	Üzemanyagellátási problémák 6 napon keresztül az USA nyugati partján és a repülőtereken	4.4M USD váltságdíj és egyéb kereskedelmi károk
Gyógyszeripar	Merck	Ransomware, NotPetya	Gyártás és értékesítés leállítás	670M USD
Szállítmányozás és Logisztika	A.P. Moller Maersk	Ransomware, NotPetya	A működés 2 hetes leállása az informatikai rendszerekhez történő hozzáférés hiánya miatt	300M USD

Mit lehet tenni?



Mit lehet tenni?

Irányítási és szabályozási terület

Feladatok		
Kiberbiztonsági kockázatfelmérés és értékelés	Naprakész Üzletmenet folytonossági (BCP) és katasztrófa-elhárítási (DRP) tervek	Rendszeres DRP tesztelés
Szabályozott szerepkörök kialakítása a rendszerekhez	Konfiguráció kezelési és változtatási folyamatok alkalmazása	A működési határértékek legyenek ismertek és dokumentáltak

Megoldások	
A belső folyamatok és szabályozások teljes áttekintése és aktualizálása	A kialakított DRP tervek rendszeres tesztelése
Külső szakértői támogatás igénybevétele a teljeskörű megoldás érdekében	

Mit lehet tenni?

Technológiai feladatok

Vagyonleltár

Eszközök nyomonkövetése

Eszközök szoftvereinek, konfigurációnak rendszeres mentése

Automatizáltan Nozomi Networks vagy Cisco Cyber Vision megoldással

Hozzáférés vezérlés

Védett módú, felügyelt és naplózott eszközhozzáférés

Cisco NAC ISE rendszer és Cisco Cyber Vision termékekkel valósítható meg

Mit lehet tenni?

Technológiai feladatok

Adatbiztonság

- Eszközök közötti titkosított kommunikáció
- Eszközök mentett szoftvereinek és konfigurációinak titkosított tárolása
- Az OT/ICS eszközök konfigurációja
- Megfelelő storage használata

Hálózati védelem

- Az OT/ICS és IT hálózatok szétválasztása tűzfallal, „légrés/airgap” kialakítása
- Hálózati forgalom monitorozása az ipari protokollokra is, kártékony kódok azonosítása
- Ipari protkollokat kezelő tűzfalak
- Nozomi Networks, Cisco Cyber Vision megoldással

Mit lehet tenni?

Technológiai feladatok

Folyamatos biztonsági monitoring

Logelemzés
- OT/ICS eszközökre
- hálózati forgalomra
- Fizikai rendszerekre

Nozomi Networks vagy Cisco Cybervision megoldással

EDR/XDR rendszerekkel

SOC szervezet
- Ügyfél oldali
- Kontron által üzemeltetve

Rendellenes események észlelése

Védett módú, felügyelt és naplózott eszközhozzáférés

Cisco NAC ISE rendszer és Cisco Cyber Vision termékekkel valósítható meg

Összefoglalva

Az OT/ICS security megfelelő tervezéssel és implementációval jól kezelhető szakmai terület

Az OT/ICS security-re kidolgozott keretrendszerek, megoldások rendelkezésre állnak

A biztonsági incidensek megelőzése jelentősen kevesebb költséggel jár, mint az utólagos kezelésük

A Kontron szállító partnerei megfelelő OT/ICS security megoldásokkal rendelkeznek

A Kontron mind az irányítási, mind a technológiai feladatokra megfelelő kompetenciával rendelkezik

NIS2 irányelv
Az EU tagállamok magas szintű kiberbiztonságáért
Határidők:
2024. Június 30. Bejelentkezés
2024. December 31. Megfelelés
2025. December 31. Az első audit határideje

Van lehetőség a kockázatok kezelésére és kézben tartására!

OT security témáról részletesebben:

- Dr. Krasznay Csaba:
  - KIBERBIZTONSÁG A XXI. SZÁZADBAN

- Nemzeti Kibervédelmi Intézet:
  - Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve

- National Institute of Standards and Technology (NIST)
  - Guide to Industrial Control Systems (ICS) Security - SP 800-82 Rev. 2 / SP 800-82 Rev. 3 (Draft)

Kontron blogpostok:

Ipari és gyártó rendszerek informatikai biztonsága operational technology security - S&T (snt.hu)

https://snt.hu/blog/ipari-halozatok-a-kibertamadok-csemegeje/

https://snt.hu/blog/ipari-halozatok-atlathatosaga-es-vedelme-ixia-es-nozomi-eszkozokkel/

https://snt.hu/blog/industry-40-network-visibility-and-protection-with-keysight-and-nozomi-devices/

Contact

Piszker György
Rendszer Architect vezető
gyorgy.piszker@kontron.hu

Kontron Hungary Kft.
2040 Budaörs Puskás Tivadar út 14/C
T: +36 1 371 8000
kontron@kontron.hu

Kontron AG
Industriezeile 35
A-4020 Linz
www.kontron.com