NIS2-kompatibilis OT védelem a gyakorlatban

Biztonságos távoli elérés, OT végpontvédelem, (mikro)szegmentáció

COM-FORTH

Valós védelem kialakítása…?

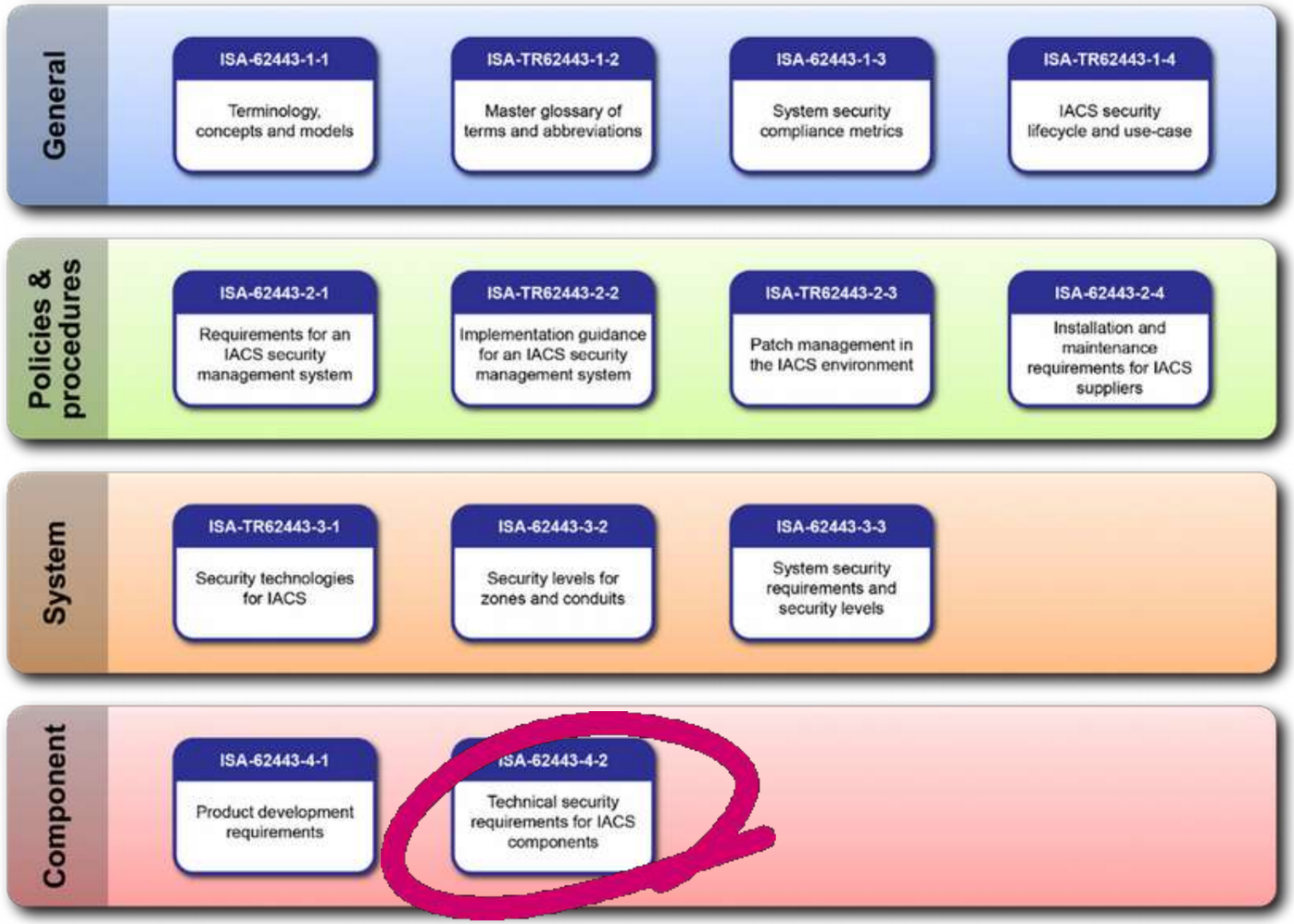
🔹 NIS2 irányelv -> Jogszabályi kényszer és felelősségi keret
- Meghatározza, mit kell elérni (kockázatkezelés, incidenskezelés, MFA, BC)
- ❌ Nem mondja meg, hogyan
- 🔹 Trigger, nem megoldás 🔹

Magyar kiberbiztonsági törvény -> A NIS2 nemzeti leképezése
- Auditálhatóság, besorolás, hatósági elvárások
- ❌ Nem OT-specifikus
- 🔹 Kötelező megfelelés, nem architektúra 🔹

NIST SP 800-82 -> OT/ICS-specifikus biztonsági iránymutatás
- Gyakorlati szemlélet, architektúra-logika, kockázatok
- ❌ Nem kötelező, nem teljes kontrollrendszer
- 🔹 Jó térkép, de nem szabvány

🔹 IEC 62443 -> OT-ra tervezett nemzetközi szabvány
- Konkrét architekturális modell (Zone & Conduit)
- Részletes technikai követelmények (FR-ek, SR-ek)
- Kockázatalapú, technológiafüggetlen
- 🔹 Ez adja a „hogyan”-t!

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

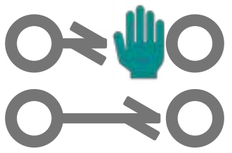
Technical security requirements for IACS components

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.

Alapvető követelmények (FR)

- Az IEC 62443 összes követelménye visszavezethető hét **alapvető követelményre** (Foundational Requirements – FR).
  A rendszereknek – és bizonyos esetekben még az egyes komponenseknek, például hálózati eszközöknek is – olyan követelményeknek kell megfelelniük, amelyek hozzájárulnak ehhez a hét alapvető követelményhez.

FR1	FR2	FR3	FR4	FR5	FR6	FR7
						
IAC	**UC**	**SI**	**DC**	**RDF**	**TRE**	**RA**
Identification & Authentication Control	Use Control	System Integrity	Data Consistency	Restricted Data Flow	Timely Response to Events	Resource Availability

1. példa: monitoring és audit

FR2: Use Control

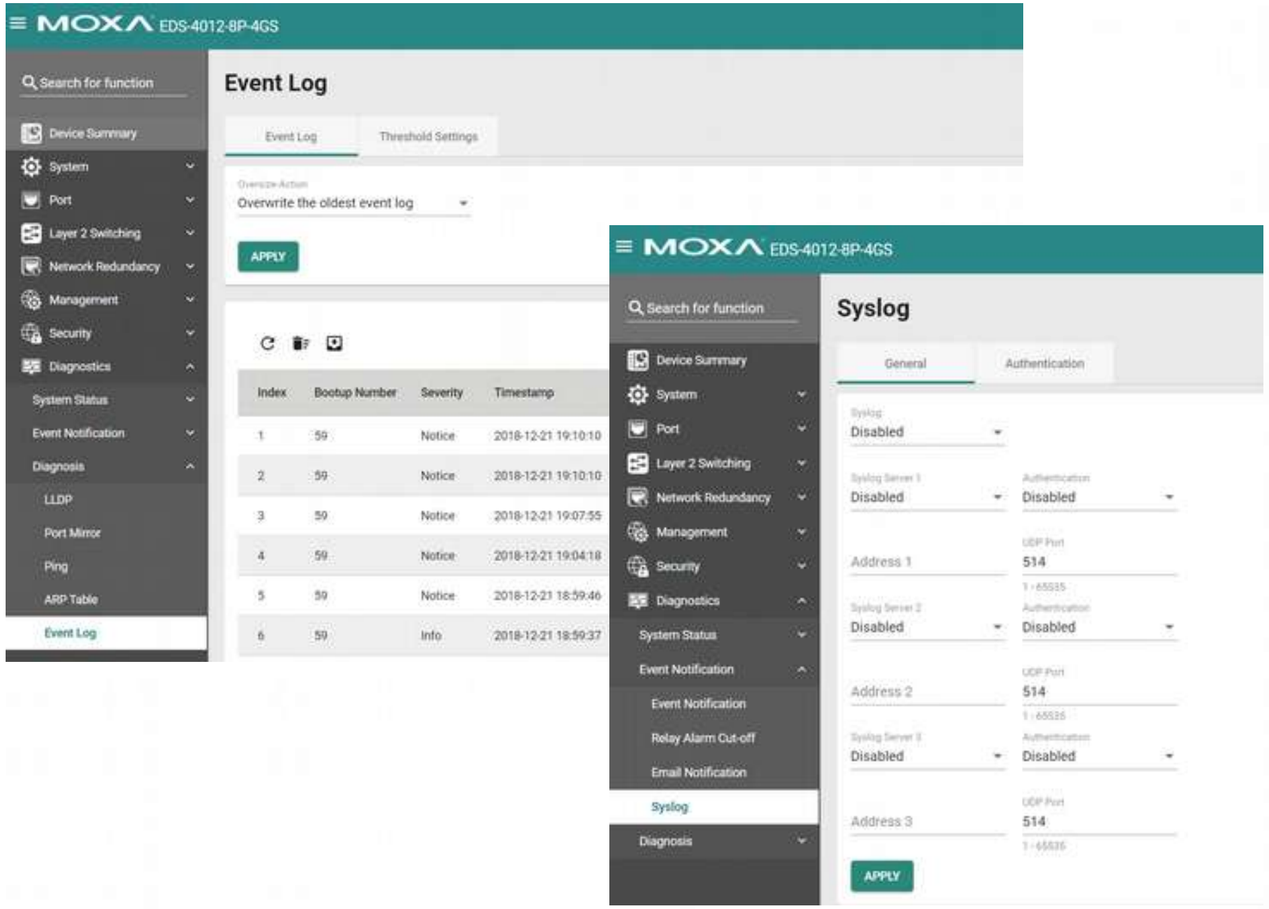
Security Level 1	CR2.8 – Auditálható események

FR6: Timely Response to event

Security Level 2	CR6.2 – Folyamatos felügyelet

1. példa: monitoring és audit

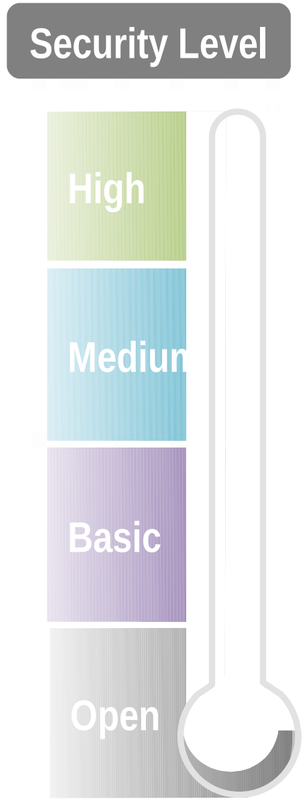
- Cél:
  - Logok gyűjtése felügyeleti és auditálási célokra
  - Annak szabályozása, hogy mely felhasználók férhetnek hozzá az információkhoz
  - Események folyamatos figyelése a gyors észlelés és reagálás érdekében
- Funkció:

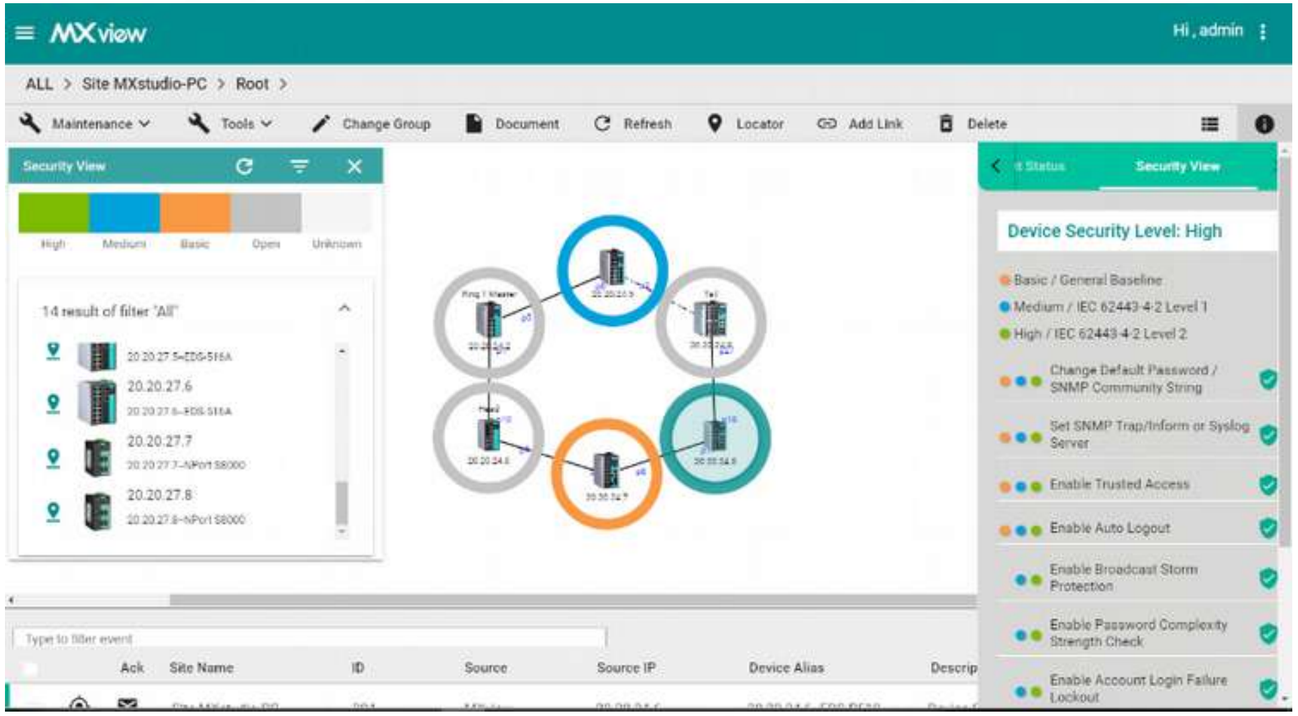


Funkciók listája biztonsági szintenként

Check Items / Built-in Profiles	High	Medium	Basic	Open	Unknown
	IEC 62443-4-2 Level 2	*IEC 62443-4-2 Level 1*	*General Baseline**		
· Enable Auto Logout	Enabled	Enabled	Enabled	-	N/A
· Set Login Message	Set	Set	-	-	N/A
· Disable Non-encrypted TCP/UDP Ports	Disabled	Disabled	-	-	N/A
· Enable Account Login Failure Lockout	Enabled	Enabled	-	-	N/A
· Enable Trusted Access	Enabled	Enabled	Enabled	-	N/A
· Enable Password Complexity Strength Check	Enabled	Enabled	-	-	N/A
· Enable Configuration File Encryption	Enabled	-	-	-	N/A
· Enable Broadcast Storm Protection	Enabled	Enabled	-	-	N/A
· Set SNMP Trap/Inform or Syslog Server	Set	Set	Set	-	N/A
· Change Default Password / SNMP Community String	Changed	Changed	Changed	-	N/A

A biztonsági szintek vizualizációja





- Biztonsági nézet
  - Vizuális áttekintés a biztonsági szintekről
  - IEC 62443-4-2 szerinti eszközvédelem
- Biztonsági varázsló
  - Egyszerű beállítás néhány kattintással az IEC 62443-4-2 szerint

2. példa: biztonságos távoli elérés

A NIS2 nem definiálja: ha van távoli elérésed, azért te felelsz, és azt kockázatalapon, megfelelő kontrollokkal kell megvalósítanod.

Az IEC 62443 ad a távoli elérésre egy architekturális keretet: zónákra bont, kontrollált adatfolyamokat definiál, és a többit ránk bízza – felelősséggel.

- A távoli elérés egy külön kockázati zóna
- Egy dedikált csatornán (conduit) keresztül történik
- Identitáshoz kötött
- Explicit engedélyezett
- Auditált és felügyelt *(de: nem definiálja, hogy kell-e szupervízió, vagy session recording)*
- Nem ad általános hálózati hozzáférést
- *Nem mondja ki, hogy mely gyártónak milyen típusú megoldásával (SDP, VPN, stb., vagy hogy cloud alapú vagy sem)*

3. példa: végpontvédelem

A NIS2 nem írja elő a végpontvédelmet, de a kockázatkezelési és incidensmegelőzési elvárásai végponti kontrollok nélkül nem teljesíthetők.
A **végpontvédelem** (pl. antivírus, alkalmazásvezérlés, fájlintegritás-ellenőrzés, host-based firewall stb.) **nincs egyetlen szóval így megnevezve** az **IEC 62443** szabványban, de **több helyen (FR és SR) is szerepel a funkciója**.

Hogyan képzeli el az IEC 62443 a végpontvédelmet?
✗ „rakjunk fel EDR-t minden PLC-re”
✓ **kockázatalapú endpoint-kontroll**, például:

- allowlisting (ami nincs engedélyezve, nem fut)
- port / service minimizálás (least functionality)
- change control + integrity monitoring
- patch *vagy* dokumentált kompenzáló kontroll
- fizikai hozzáférés korlátozása (igen, ez is endpoint security)

TXOne Stellar: OT-natív végpontvédelem

- Legacy op. rendszer támogatás (Win2000-től)
- Újraindítás nélkül, 7/24 üzemre tervezve
- Minimális erőforrásigény
- Alkalmazások korlátozása
- USB kontroll

txOne networks

OTCCC | OT Cybersecurity Competence Center

Hálózati szegmentáció – L2 VLAN, Port Security

A VLAN-tagságot a switchport konfigurációja határozza meg – nem az IP-cím

- **Gyors, alacsony késleltetésű izoláció**
- **Kompatibilis régebbi OT-eszközökkel, nem kell IP-címeket átállítani**
- **Hibás trunk/NAT beállítás VLAN hoppingot eredményezhet**
- **L2 védelem nem lát bele az alkalmazásszintű forgalomba**
- **Menedzsment bonyolódik, ha sok VLAN-t kell karbantartani**

Pl.:
Egy PLC és egy HMI külön VLAN-ba kerül, de ugyanazon switchen.→ Megakadályozza, hogy broadcast üzenetek (pl. Profinet Discovery, ARP) átjussanak

Zones and Conduits Requirement

L3 szegmentáció — Subnet, Routing, ACL

Logikai elválasztás IP-tartományok és routing alapján

- **ACL-ekkel szabályozható a forgalom forrás/cél IP és port (L4) szerint**
- **VLAN ≠ IP: az IP-átírás nem visz másik VLAN-ba**
- **Ha több subnet él ugyanazon L2 hálózaton, az IP-módosítás biztonsági rés lehet**
- **ARP/DHCP védelem (DAI, Snooping, IP Source Guard) szükséges**
- **OT-ben címzésváltás nehézkes lehet (statikus IP-k)**
- **Nem lát bele a forgalomba (protokoll szinten)**

Pl.:

IT–OT subnet ACL-lel elválasztva; külön VLAN esetén IP-csere nem ad plusz jogot

Zones and Conduits Requirement

L7 szegmentáció — Bridge tűzfal (Transparent Firewall) — OT környezetben

Transparent mód: nem kell IP-cím vagy VLAN módosítás

- **L3–L7 szintű forgalomszűrés – protokoll alkalmazás, parancs szinten, Deep Packet Inspection (mély csomagelemzés)**
- **Ideális régi OT hálózatba; zóna–zóna védelem (IEC-62443)**
- **Inline módban: hibás konfiguráció forgalom-kiesést okozhat**
- **Költségesebb, de magasabb biztonsági szintet ad, IDS, IPS, Virtual Patch**

Pl.:
Egy TxOne EdgeIPS tűzfal az OT switch és a PLC közé kerül.
→ Átereszt minden Modbus TCP „read” kérést, de blokkolja a „write” parancsokat és a tanulási időszak alatt nem “látott” IP-ket.

Zones and Conduits Requirement

KIK VAGYUNK MI?

MAGYAR TULAJDON

100%-BAN CSALÁDI

TÖBB MINT 35 ÉVE

35

STABIL PÉNZÜGYI HÁTTÉR

TAPASZTALT SZAKEMBEREK

IPAR 4.0 SPECIALIZÁCIÓ

KÖSZÖNÖM A FIGYELMET!

Bóna Péter
CEO,
tulajdonos

MOBIL: +36-30-2007239

EMAIL: pbona@comforth.hu

WEBOLDAL: www.comforth.hu

COM-FORTH
IPARI INFORMATIKA