



ALVERAD
TECHNOLOGY FOCUS

NIS2

**IT és OT rendszerek
sajátosságai a NIS2 árnyékában**

2024.11.21.



Alverad Technology Focus Kft.

Akkreditált kiberbiztonsági vizsgálólaboratórium

- **Akkreditációk:**

- Iparbiztonság
- Szoftver és alkalmazás biztonság
- Hardver biztonság
- IT biztonság



IGAZSÁGÜGYI
MINISZTERIUM



NEMZETI
BIZTONSÁGI
FELÜGYELET



Miniszterelnökség

Iromány száma: **T/9716.**

Benyújtás dátuma: **2024-10-29 22:44**

Parlex azonosító: **PW6612AB0001**

Címzett: **Kövér László, az Országgyűlés elnöke**

Tárgy: **Törvényjavaslat benyújtása**

Benyújtó: **Dr. Semjén Zsolt, miniszterelnök-helyettes**

Előadó: **Rogán Antal, Miniszterelnöki Kabinetirodát vezető miniszter**

Törvényjavaslat címe: **Magyarország kiberbiztonságáról**

A Kormány nevében benyújtom Magyarország kiberbiztonságáról szóló törvényjavaslatot.

- (1) A 92. § az Alaptörvény 46. cikk (6) bekezdése alapján sarkalatosnak minősül.
- (2) A 96. § az Alaptörvény IX. cikk (6) bekezdése alapján sarkalatosnak minősül.
- (3) A 109–111. § és a 113. § az Alaptörvény 23. cikke alapján sarkalatosnak minősül.

Megfelelőség értékelés - audit

Helyszíni ellenőrzés

- Technológiai képességek ellenőrzése

- Biztonsági folyamatok áttekintése

- Szabályozások feljegyzések áttekintése

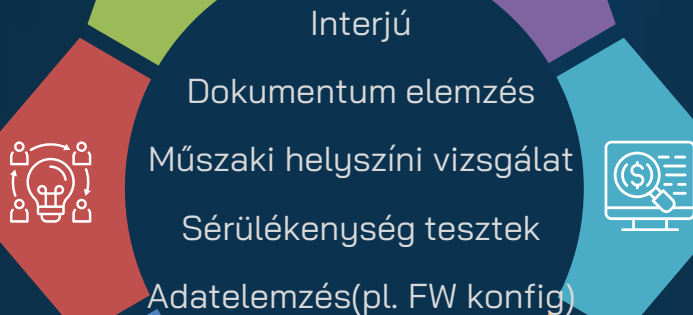
Dokumentáció ellenőrzés

Ellenőrzés előkészítése

- Hatókör áttekintése

- Kockázatértékelés áttekintése

- Osztályba sorolás áttekintése



Audit ütemezés

Nyilvántartásba
vétel



T0

Megállapodás az
auditorral



T0 + 120nap

<https://sztfh.hu/nyilvantartasok/auditorok/>

1. kiberbiztonsági
audit



T0 + 2 év

Purdue-modell

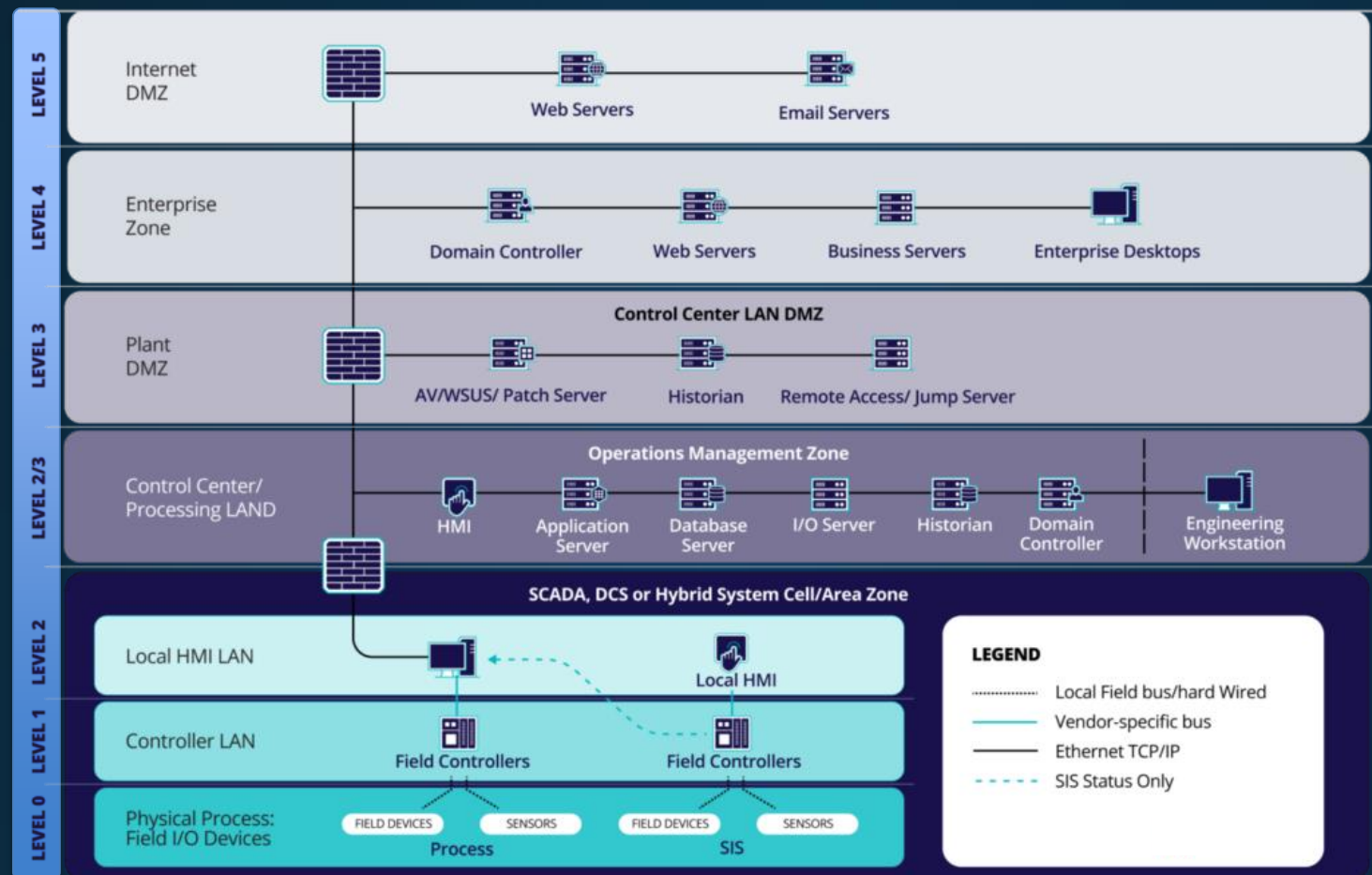
A Purdue-modell, az ipari vezérlőrendszerek (ICS) biztonságának alapvető keretrendszere.

1990-es években kifejlesztett hierarchikus modellje a komplex ICS-környezetet különálló zónákra vagy szintekre szervezi. Mindegyiknek sajátos biztonsági szempontjai vannak.

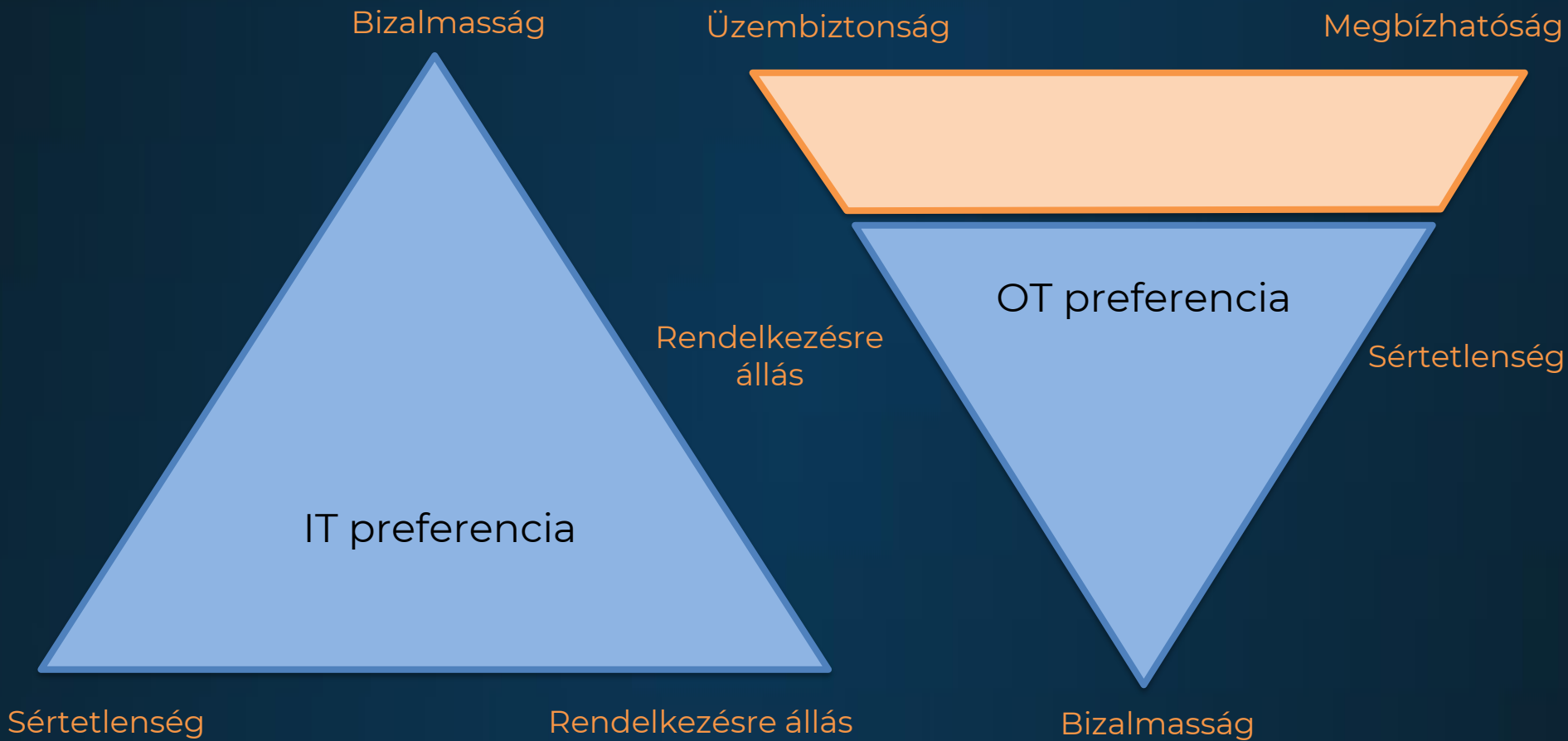
Strukturált megközelítés leegyszerűsíti:

- a hálózattervezést,
- felügyeletet
- kommunikációt,
- javítja az ipari működés biztonságát és rugalmasságát.

Elektronikus Információs Rendszer – OT rendszer (is)



IT ≠ OT



IT ≠ OT

Information Technology (IT)

Operational Technology (OT)

Összetevők, komponensek

Szerverek, munkaállomások, adattárak, felhő, biztonsági eszközök, mobileszközök, 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 konceptió

„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 (outsourc) partnert.

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

Elhelyezkedés

Centralizált rendszerek, szerverszobákban, adatközpontokban,

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

IT $\neq$ OT



Az USB kapcsolat nem monitorozható és ellenőrizhető.

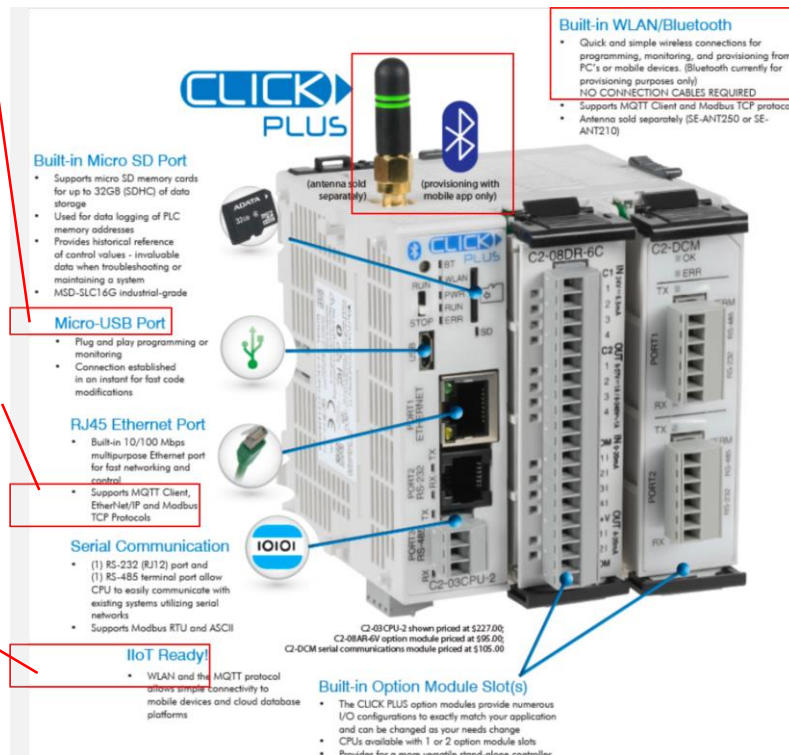
Az USB-n keresztül az eszköz konfigurációja módosítható lehet, programletöltésre van lehetőség.

Az USB kapcsolaton keresztül módosítható a program.

A MODBUS és az Ethernet/IP protokollok nem tartalmaznak kiberbiztonsági funkciókat.

- Lehallgatás
- Adatmódosítás a hálózati forgalomban
- Visszajátszás (Replay Attack)
- Jogosulatlan, hitelesítetlen hozzáférés, DOS, stb.

Hálózati szegregációs (pl. Prudue model) elvek ellehetetlenülése, közvetlen internet kapcsolat, stb.



A rádiós átviteli közeg kiberbiztonsági szempontból nem megbízható. Nyílt hozzáférésű kommunikációs csatorna.

Csak WPA2-AES PSK kapcsolódás, hitelesítés hiánya (WPA2-Enterprise kellene)

- Jogosulatlan eszközhozzáférés lehetősége Wi-Fi és BT rádiókon keresztül
- Jogosulatlan programletöltés lehetősége
- Jogosulatlan programmódosítás lehetősége
- Jogosulatlan átkonfigurálás lehetősége
- Rádiós DOS/DDoS lehetősége
- Hozzáférés-megtagadás kikényszerítése, stb.

Minden felhasználói kényelmi funkció = kockázat

De ha ismerjük a kockázatokat, képesek lehetünk olyan védelmet kialakítani, amely elfogadható szintig csillapítja a kockázatokat.

- **Ki kell vágnotok az erdő leghatalmasabb fáját ezzel a kis heringgel!**

- Ahol korábban nem foglalkoztak az OT kiberbiztonsággal, alapjaitól kell újra gondolni a hálózati infrastruktúrát és a védelmi intézkedéseket.
 - Hálózati eszközök
 - Szegmentáció
 - Zónakontroll és zónavédelem
 - Redundancia és HA
 - Hálózatvédelem
 - Protokollvédelem
 - Sérülékenységek
 - Javítások
 - Felügyelet, monitoring
- És ez még csak a hálózat...

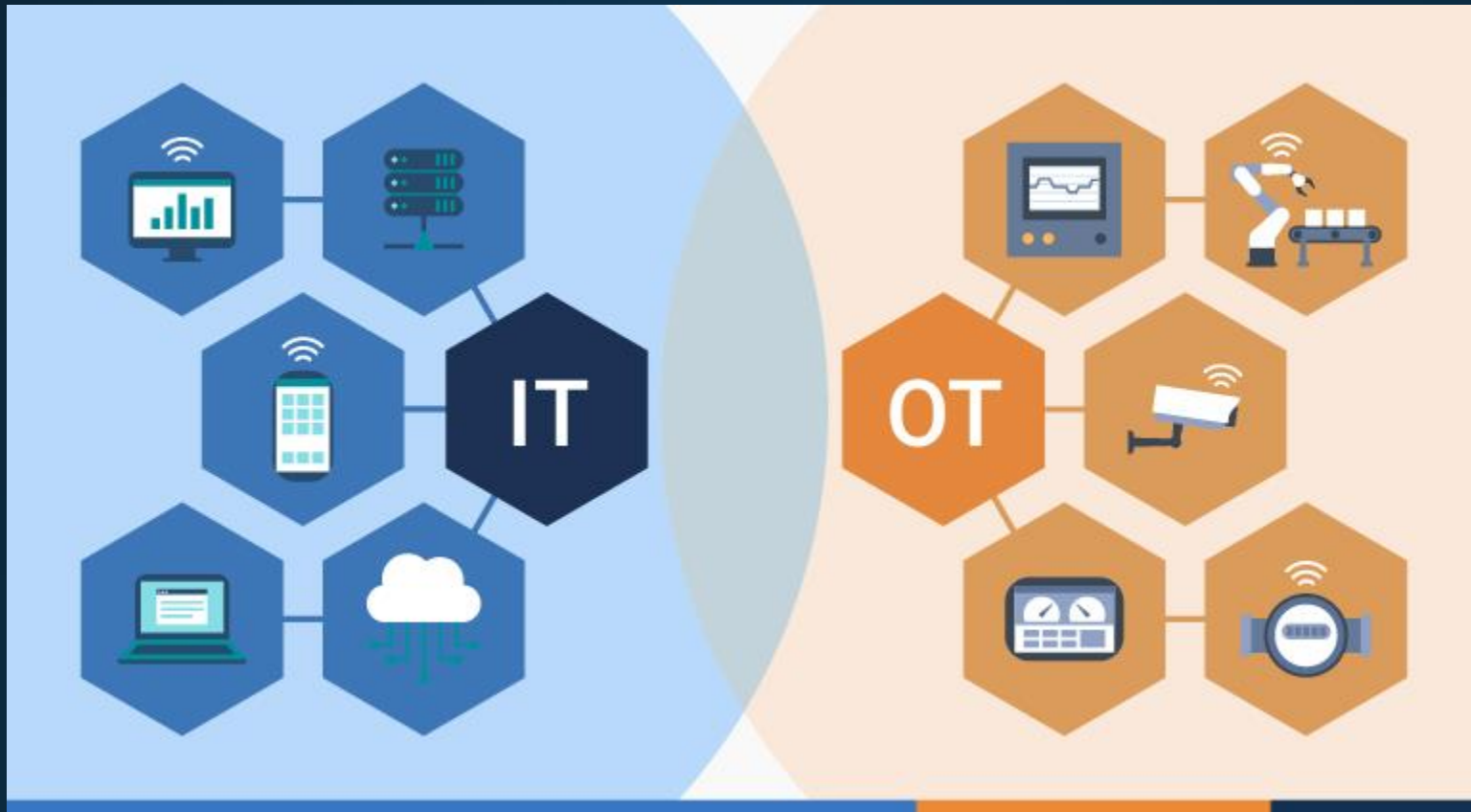


Hering

(az OT kiberbiztonság rendelkezésre álló erőforrása)

IT ≠ OT - egységes értékelés ?

IT: NIST 800-53

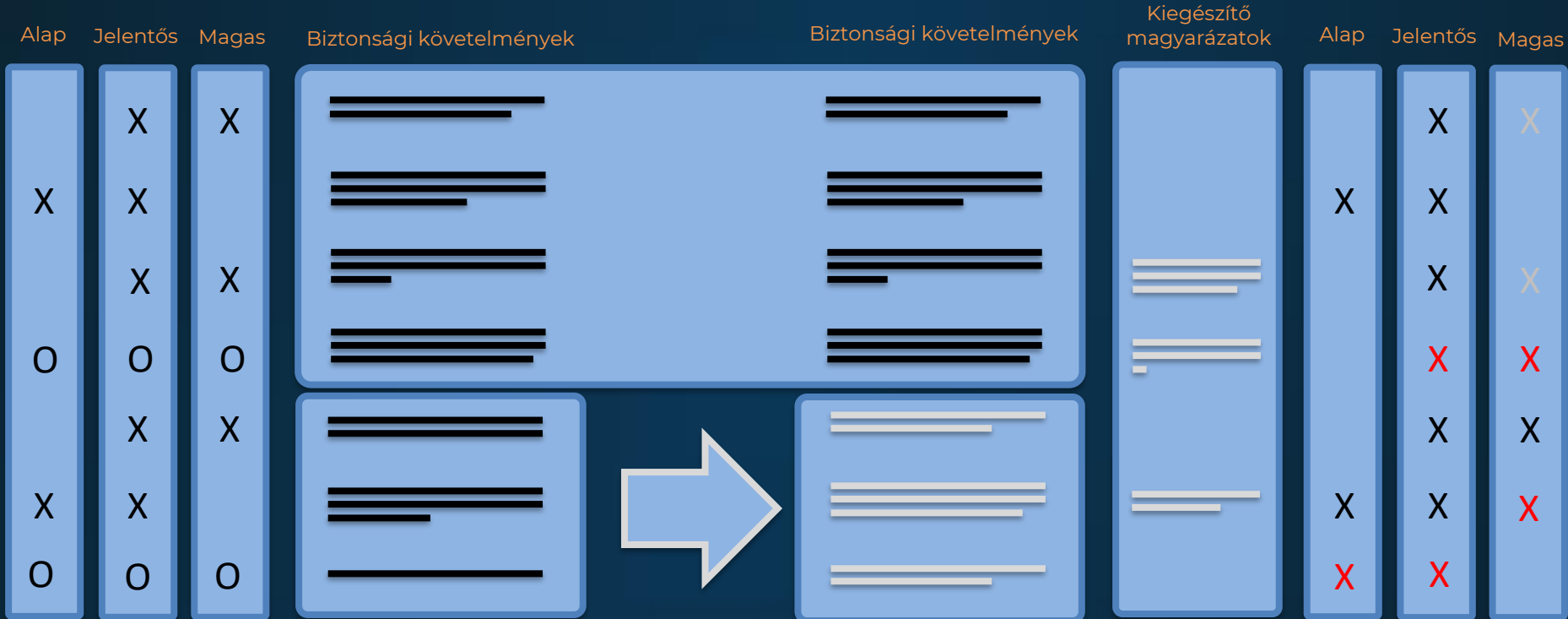


OT: NIST 800-82

IT $\neq$ OT - egységes értékelés !

IT: NIST 800-53

OT: NIST 800-82



Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

IT: NIST 800-53

- › Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.

OT: NIST 800-82

- › Amennyiben az EIR nem támogatja a naplóbejegyzések gyűjtését, a naplóbejegyzések felülvizsgálatát az EIR rendszerbiztonsági tervében meghatározott rendszerességgel manuális ellenőrzéssel kell végezni.
- › **Magyarázat:** A helyettesítő védelmi intézkedések magukba foglalhatják például a kézi mechanizmusokat vagy eljárásokat. Olyan eszközök esetében, ahol a naplóbejegyzések gyűjtését nem tudják megvalósítani, időszakos manuális felülvizsgálatra lehet szükség.

Eszköz zárolása

IT: NIST 800-53

- › Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést.

OT: NIST 800-82

- › Abban az esetben, ha az EIR nem rendelkezik automatikus zárolási képességgel, vagy vészhelyzetben azonnali kezelői reakcióra van szükség, ezért zárolással nem lehet megakadályozni az EIR-hez való hozzáférést, a szervezet kockázatértékelés alapján helyettesítő intézkedést vezet be, amelyet dokumentál az EIR rendszerbiztonsági tervében.

Az elektronikus információs rendszer helyreállítása és újraindítása

IT: NIST 800-53

- › Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

OT: NIST 800-82

- › Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.
- › **Magyarázat:** Az érintett szervezet megvizsgálja, hogy az EIR utolsó ismert, üzembiztos állapotba történő helyreállításakor a felmerülő kockázatok figyelembevételével a rendszer állapotváltozóit vissza kell-e állítani a kezdeti értékekre vagy az üzemszünet előtti értékekre.

Behatolásvizsgálat (penetration testing)

IT: NIST 800-53

- Az érintett szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken

OT: NIST 800-82

- Az érintett szervezet az OT funkciók zavartalanságának biztosításával behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.
- **Magyarázat:** A behatolásvizsgálatokat megfontoltan alkalmazzák az OT-hálózatokon, hogy az ellenőrzési folyamat ne befolyásolja hátrányosan az OT-funkciókat. Az OT-rendszerek általában nagyon érzékenyek az időzítési korlátokra, és korlátozott erőforrásokkal rendelkeznek. A helyettesítő ellenőrzések közé tartozik például a replikált, virtualizált vagy szimulált rendszer alkalmazása a behatolásvizsgálat elvégzéséhez. Előfordulhat, hogy a tesztelés elvégzése előtt le kell állítani a gyártás alatt álló OT rendszert. Ha az OT-rendszereket tesztelés céljából lekapcsolják, a tesztek lehetőség szerint a tervezett OT leállások idejére kell ütemezni. Ha a behatolásvizsgálatot nem OT-hálózatokon végzik, fokozottan ügyelni kell, hogy a tesztek ne terjedjenek át az OT-hálózatra.

10 – 25 év

Kerülő megoldások



- Architektúrák
- Komponensek képességei
- Szemléletmód
- Fehér és kék galléros párbeszéd

Beépített biztonság



Köszönöm a figyelmet!

- Répás József
- Repas.Jozsef@alverad.hu