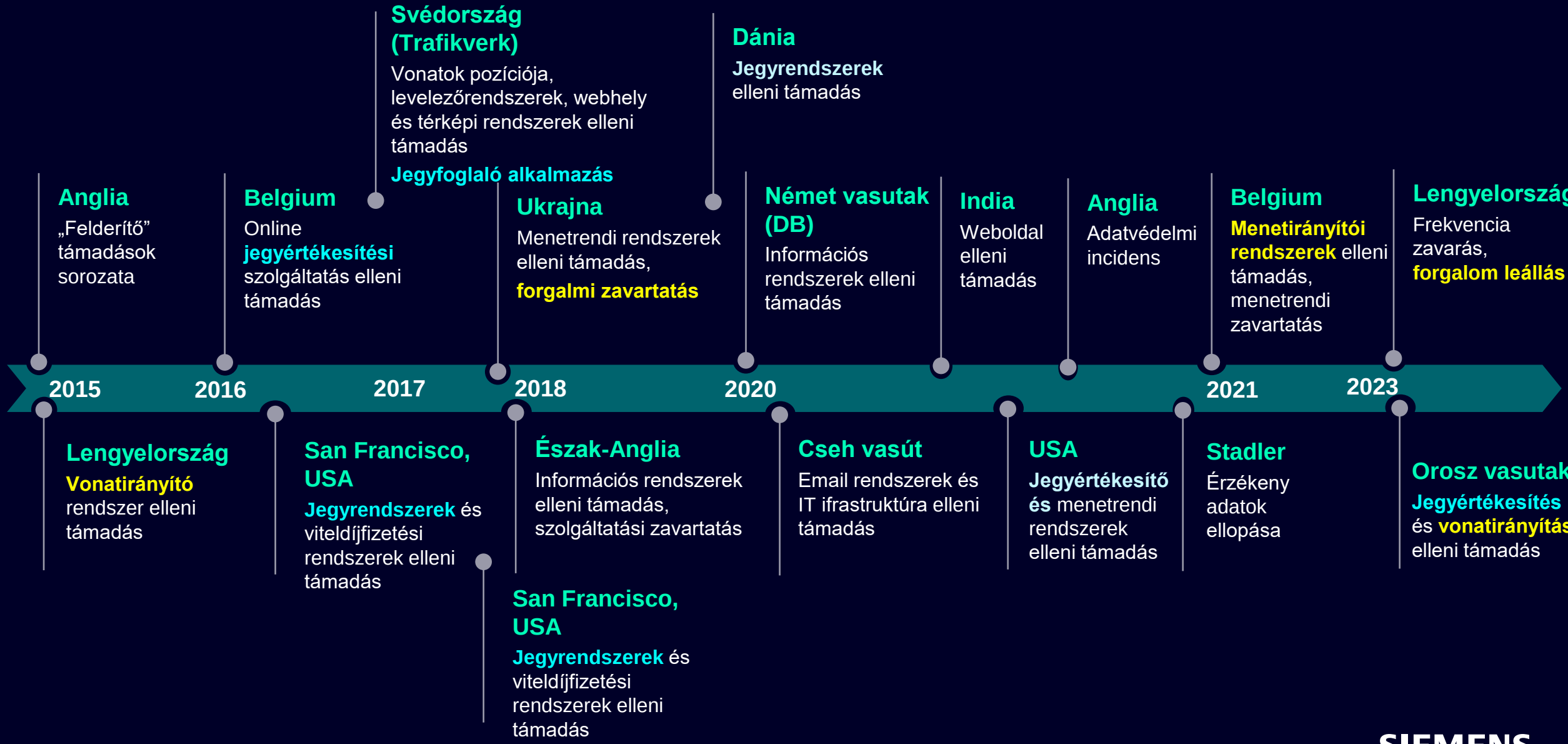
Kiberbiztonság a vasúti rendszerekben [NIS 2]

XXIV. Közlekedésfejlesztési és beruházási konferencia

Bükfürdő, 2024. április 17.

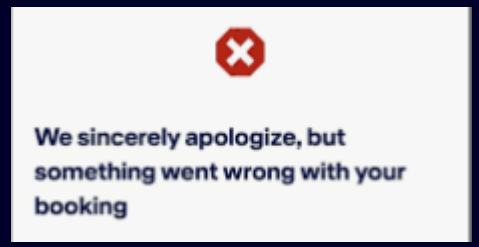
SIEMENS

Kibertámadások a vasúti szektorban



SIEMENS

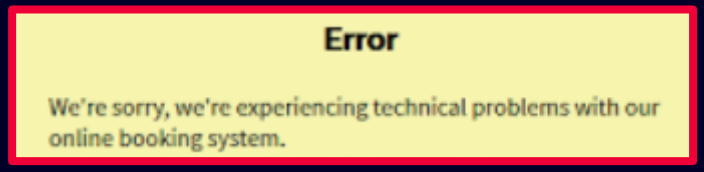
Támadások jellege a vasúti szektorban



Zsaroló program (ransomware) 45%

Adatvesztéshez, kiadáshoz köthető fenyegetések

Szolgáltatás megtagadással járó támadás (DoS) = túlterheléses támadás
Elosztott szolgáltatásmegtagadással járó támadás (DDoS) 25%



Behatolás, ismert IT sebezhetőségek kihasználása 15%

Csalás, hamisítás, ellátási lánc elleni támadás 5-5%

SIEMENS

Szabályzás és szereplők

NIS irányelv (2016/1148 EU)
Hálózatok és információs rendszerek biztonságáról szóló irányelv – bejelentési szabályok

„Kritikus infrastruktúra” – alapvető szolgáltatók

- Telekommunikációs szektor
- Energia szektor
- Digitális, hálózati, internet infrastruktúra
- Egészségügy
- Pénzügyi szektor
- Hajózási szektor
  Légi közlekedés
- **Vasúti szektor**

Alapvető szolgáltatások üzemeltetői (OES)

- **Vasúttársaságok** (2012/34/EU irányelv szerint)
- **Pályahálózat-működtetők** (2012/34/EU irányelv szerint)
- **Ellátási lánc (beszerzés)**
- **Szállítási lánc (fuvarozás, logisztika)**
- **Szolgáltatók**
- **Hatóságok és szervezetek**
- **Közterületek (utasváró, étterem)**
- **Egyéb szervezetek (bank, fuvarbiztosítás)**

nemzeti szabályozási keret

- **VT és PM**
- **Áru és Személyszállítás**
- **Alapvető vasúti szolgáltatások**
  - Hálózat üzemeltetés
  - Hálózati kapacitás elosztás, speciális szállítmányok (veszélyes áru)
  - Vasúti infrastruktúra és vonatok beszerzése, üzemeltetése, karbantartása
  - Áru- és utasszállítás
  - Utasok és áruk biztonsága, védelme
  - Jegyértékesítés
  - Utas és ügyfél tájékoztatás
  - Számlázások, pénzügy
  - Erőforrások, rendszerek

Útmutatás, ajánlás, támogatás;
Események szervezése,
Szabványosítási törekvés

Tudatosság
Általános biztonsági szint
Eltérő tagállami végrehajtási szint

SIEMENS

NIS 2 irányelv (2022/2555 EU) I.

Célja:

- **A kiberbiztonság közös, magas szintjének elérése az EU-n belül, a belső piac működésének javítása mellett**
- **A kiberbiztonsági követelmények és a kiberbiztonsági intézkedések végrehajtása terén mutatkozó eltérések, hiányosságok megszüntetése a különböző tagállamokban**
- **Kiberbiztonsági intézkedések a kritikus ágazatokban (szélesebb kör, hatósági szabályzás)**
- **Tagállami jogalkotás határideje: 2024. október 17.**
- **Kritikus és kiemelten kritikus kategóriájú ágazati szolgáltatók** (2025. április 17.)
- **Tagállami szerepvállalás előírása:**
  - **Kiberbiztonsági nemzeti stratégia** (célok, erőforrások, szakpolitikai és szabályozási intézkedések)
    - Polgári tudatosság általános szintjének fokozása
    - Kiberbiztonsági tanúsítás
    - Követelmények beillesztése a közbeszerzésekbe
    - **Felelős illetékes hatóság** megnevezése
      - Kötelező erejű utasítások (esemény megelőzéséhez, orvosláshoz, végrehajtási folyamatok határideje, stb) Irányelvek végrehajtásának felügyelete, ellenőrzése
      - Egyedüli kapcsolattartó pont – határon átnyúló együttműködésben, Bizottsággal, ENISA-val
      - Kiberbiztonsági események és válságok kezelése, intézkedések értékelése
    - **CSIRT :** nemzeti számítógépes biztonsági eseményekre reagáló csoport

ENISA – **Uniós kiberbiztonsági jelentés** (két évente): kockázatértékelés, fenyegettségi helyzet, tudatosság szintje, érettségi szint, szakpolitikai ajánlások

NIS 2 irányelv (2022/2555 EU) II.
FONTOS KÖTELEZETTSÉGEK ÉS ELVÁRÁSOK

Kockázatkezelési intézkedések : minden műveletre kiterjedő kiberbiztonsági kockázatértékelés elvégzése és megfelelő és arányos intézkedések bevezetése *21.cikk*

→ **Hálózati és információs rendszerek, valamint e rendszerek fizikai környezetének védelme**

- Kockázatelemzési és kockázatkezelési szabályzatok → **a kockázatkezelési kultúra előmozdítása**
- Üzletmenet-folytonosság, tartalékrendszerek, helyreállítás, válságkezelés
- Ellátási lánc biztonsága, humán erőforrás biztonsága, hozzáférési szabályok, vészhelyzeti kommunikáció

- Késedelem nélküli **jelentéstételi kötelezettség súlyos (jelentős) esemény esetén** *23.cikk*
  - súlyosság (működési zavar, vagyoni- és nem vagyoni saját vagy harmadik fél számára okozott kár) alapján
  - korai előjelzés, első bejelentés (24 óra), eseménybejelentés (72 óra), zárójelentés (egy hónap)
- Tanúsított termékek, szabványosításra törekvés *25.cikk*
- Kiberbiztonsági információ megosztási megállapodás (önkéntes alapon) *29.cikk*

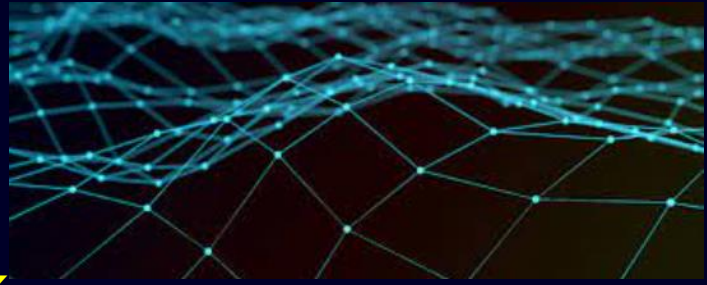
  OES - > tagállami szint -> ENISA tanácsadás, útmutatás
- **Irányítói, vezetői felelősség : jóváhagyás, végrehajtás felügyelet, képzések, felelősségre vonhatóság** *20.cikk*

Közigazgatási bírság kiszabása: 10 millió EUR vagy 2% éves globális forgalom kiemelten kritikus ágazat esetében a 21. és 23. cikk megsértése esetén

SIEMENS

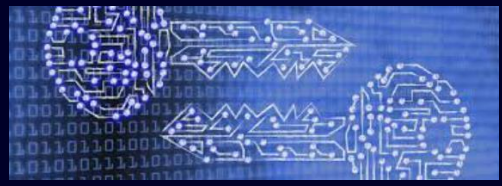
Elvárt kockázatcsökkentő *intézkedések* a gyakorlatban NIS 2

„minden veszélyre kiterjedő megközelítés”



Célja a a hálózati és információs rendszereknek és azok fizikai környezetének a védelme, a szolgáltatások rendelkezésre állása, hitelessége, integritása vagy bizalmas jellege megőrzése érdekében.

- Kockázatelemzési – és eseménykezelési stratégia
- Üzletmenet-folytonosság (üzemzavar alatt és után), katasztrófa helyreállítás, válságkezelés



- Ellátási lánc biztonsága (közvetlen beszállítók)
- A kiberbiztonság ellátási láncától való függés
- Biztonsági koncepció a hálózatok és információs rendszerek vásárlására, fejlesztésére, használatára, karbantartására, a sebezhatőség felderítésére
- Irányelvek a kiberkockázat kezelés hatékonyságának felmérésére

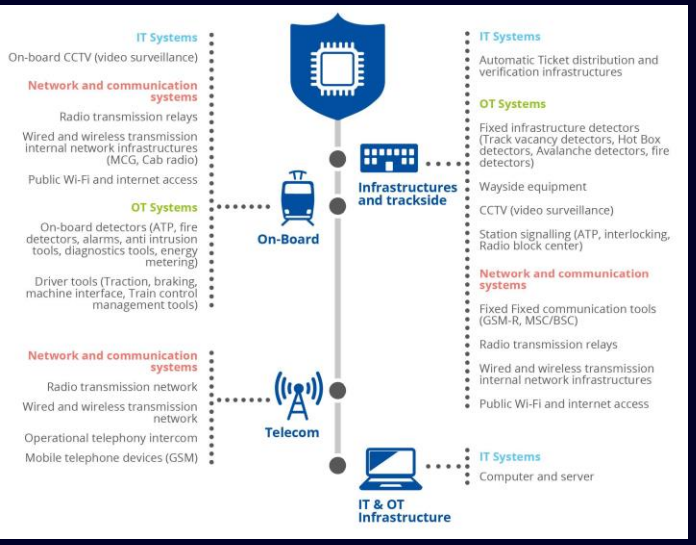
- Kiberhigiéniai gyakorlat és képzések
- Személyzeti hozzáférés szabályzása
- Biztonságos kommunikációs csatornák, több-faktoros azonosítási rendszerek, kriptográfia használata

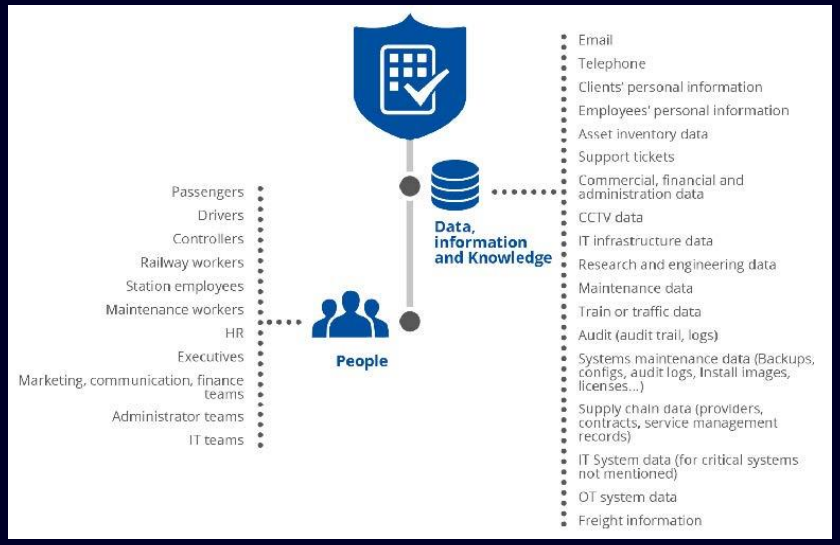
- Vészhelyzeti kommunikáció irányelvei

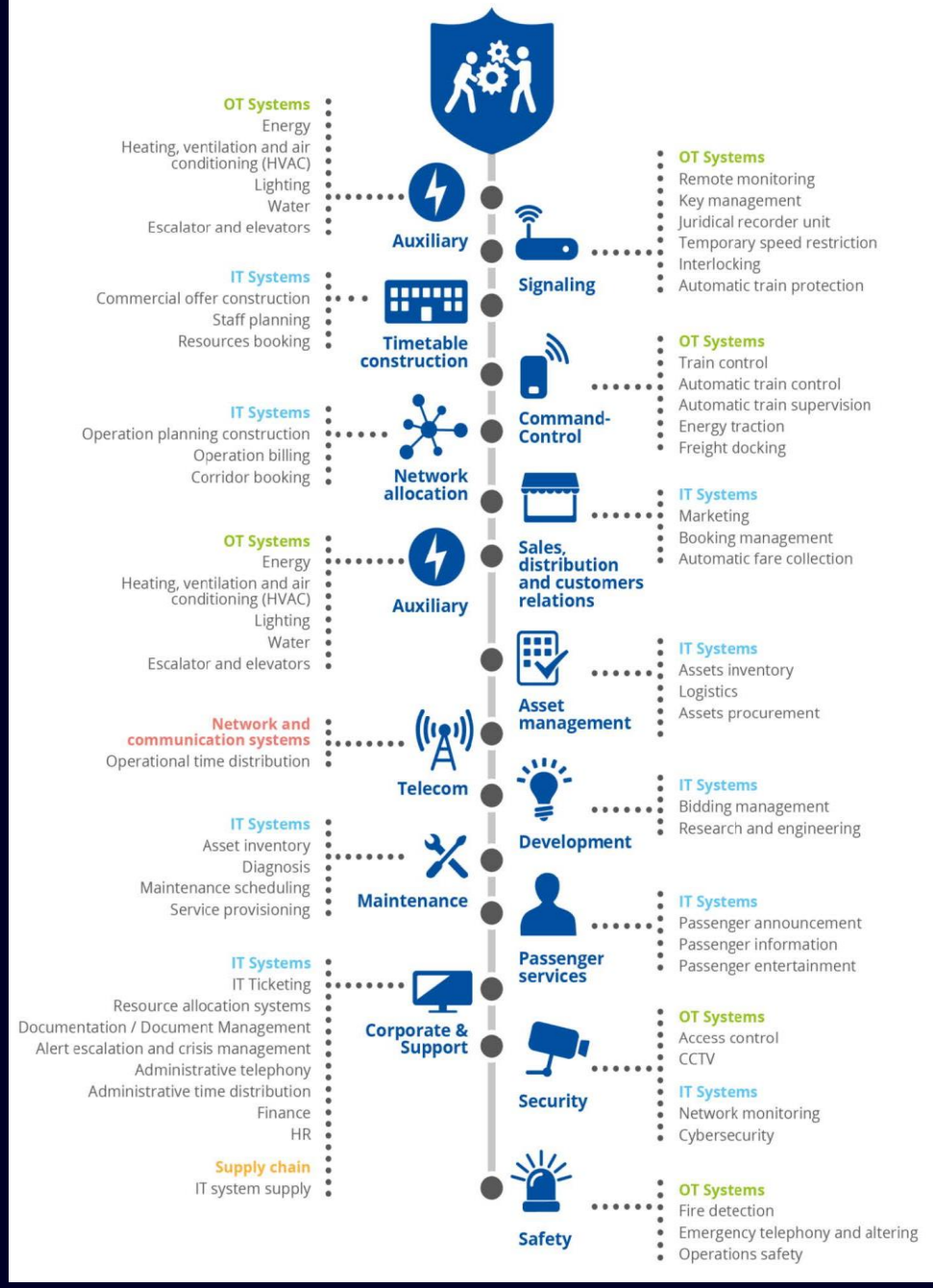
SIEMENS

A vasúti szektor kiberbiztonsági kihívásai (EU felmérés)

- Alacsony (de lassan növekvő) digitális és kiberbiztonsági tudatosság
- Nehézségek az operatív biztosítóberendezési és a kiberbiztonsági világ összeegyeztetésében
- A vasúti infrastruktúra földrajzi elterjedése és az örökölt rendszerek megléte
- A vasúti alaptevékenység digitális átalakítása
- A kiberbiztonság ellátási láncától való függés, beszállítók kategórizálása
- A biztonság, a versenyképesség és a működési hatékonyság egyensúlyának igénye, a kiberbiztonság költségvetési egyensúlya
- A kiberbiztonsági szabályozások összetettsége







SIEMENS

Kiberkockázati forgatókönyvek

- Jelzőrendszer vagy az automatikus vonatvezérlő rendszer veszélyeztetése

  Alacsony valószínűség + nagyon nagy lehetséges hatás




- Célzott támadás (pl ipari vezérlőrendszer alkalmazásá
  rendszerek szabotálására
- Zsarolószoftver támadás in
  tevékenység me varás
- Ügyfe adatai
  da sze
  piacon
  en ke
  at kiszivárogtatás
  ttált es ok hálózatán keresztül, nagymennyiségű
  pl. a jegyértékesítési rendszerek lebénítására
- esemény általi, fizikai informatikai rendszer megsemmisülés, a
  gáltatási tevékenység megzavarása

Rendszer életkora
Rendszer tervezése
Rendszer karbantartása

→ Sérülékenységek száma és súlyossága

→ Pénzügyi veszteség
Biztonság
Hírnév károsodása

Kiberbiztonsági kockázatértékelési módszerek

- Hiányértékelés
- Érettségi felmérés
- Sebezhetőségi felmérés
- Penetrációs teszter bevezetése
- Belső auditok
- Automatizált eszközalapú biztonsági tesztek

ISO27001
ISO27005
IEC62443
CLC50701

A fenyegetési forgatókönyv valószínűségének felmérése

Különböző kiberkockázat-kezelési keretrendszerek:

- CVCC (általános sérülékenységi pontozási rendszer) kihasználhatósági mérőszámok

  Támadási vektor (rendszer expozíció),

  Támadási összetettség,

  Szükséges jogosultságok,

  Felhasználói interakció
- Fenyegetés előfordulásának valószínűsége, a kitettség könnyűsége és az eszköz értéke

Biztonsági kockázat = (valószínűség) x hatás = (fenyegetések x sérülékenységek) x hatás

Vasúti kiberbiztonsági keretrendszer (SIEMENS adaptáció)

Solutions for railways

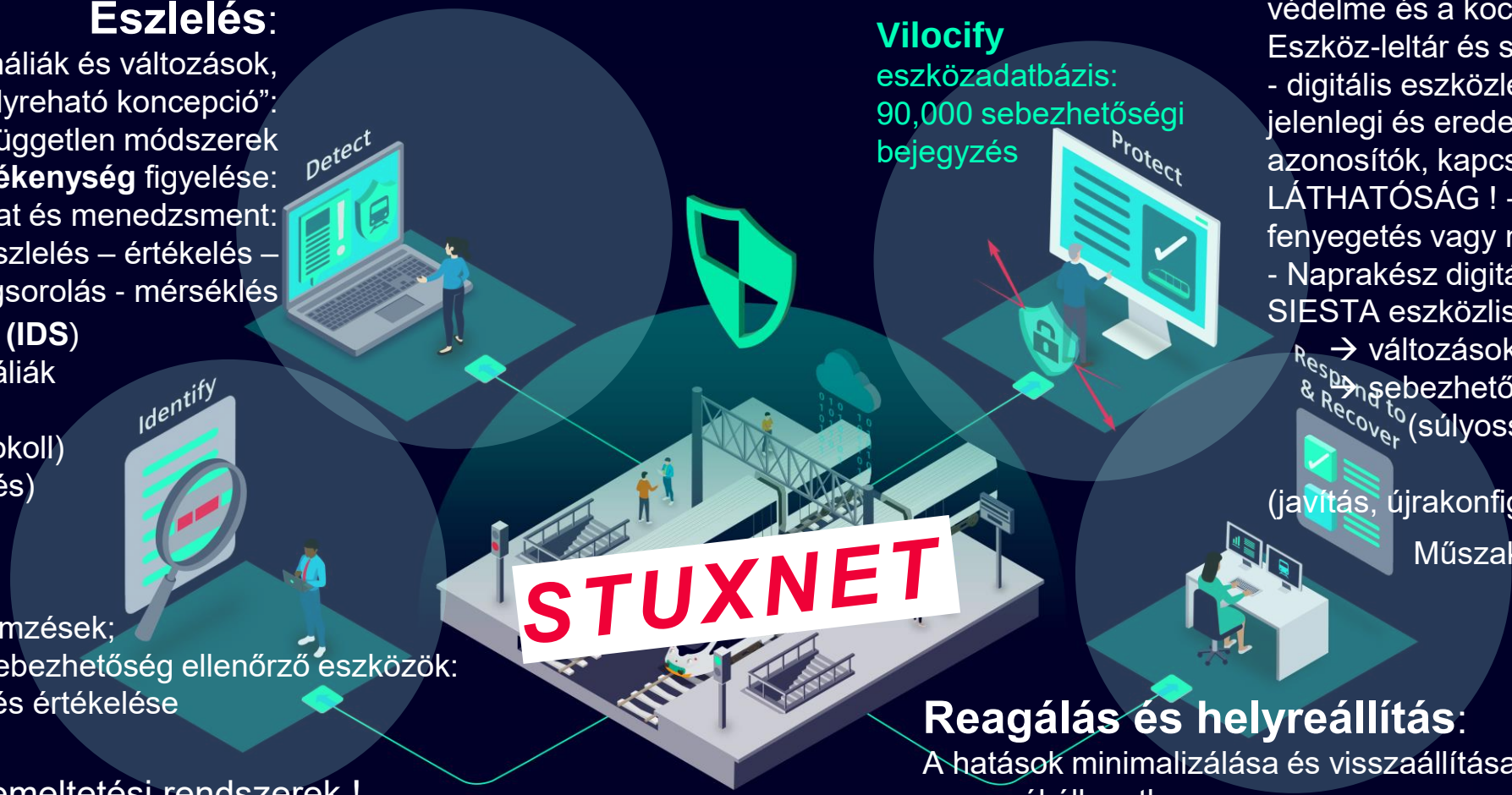
Észlelés:

Anomáliák és változások,
„Mélyreható koncepció”:
független módszerek
Szoftveres **sérülékenység** figyelése:
Érzékenységvizsgálat és menedzsment:
korai észlelés – értékelés –
rangsorolás - mérséklés

Behatolásvizsgálat (IDS)
– támadások, anomáliák
észlelése:
- aláírás-alapú (protokoll)
- AI alapú (viselkedés)

Azonosítás:

Üzleti veszélyek és
biztonsági rések, elemzések;
Eszközfelderítő és sebezhetőség ellenőrző eszközök:
penetrációs tesztek és értékelése



Vilocify
eszközadatbázis:
90,000 sebezhetőségi
bejegyzés

Védelem:

A kritikus rendszerek(vasútüzem)
védelme és a kockázatok csökkentése
Eszköz-leltár és sebezhetőség kezelés:
- digitális eszközleltár: vagyontárgyak
jelenlegi és eredeti állapota (verziók,
azonosítók, kapcsolódások) ->
LÁTHATÓSÁG ! ->
fenyegetés vagy normális viselkedés?
- Naprakész digitális eszközadatbázis +
SIESTA eszközlista
→ változások nyomon követése
→ sebezhetőségi riasztások (CVCC)
(súlyosság, kihasználhatóság)
→ döntés
(javítás, újrakonfigurálás, szegmentálás)

Műszaki megoldások
- NAC
- adattitkosítás,
- tűzfalak,
- adatdiódák (DCU

Reagálás és helyreállítás:

A hatások minimalizálása és visszaállítása
a normál állapotba;
Reagálási terv – üzletmenet folytonossági
terv – működési folytonosság terv –
válságkommunikációs terv
Tréningek, oktatás,
Tudatosság felépítése

SIESTA:
- kritikus üzemeltetési rendszerek !
- egyetlen felhasználói felület, biztonságos vezérlés
- egyedileg összeállított vizsgálati eljárások, jóváhagyott teszt esetek
- rendszeres tájékoztatás a biztonsági állapotról
- strukturált és vizualizált jelentés a lehetséges fenyegetésekről és sebezhetőségről

SIESTA (Siemens Extensible Security Testing Appliance)

SIEMENS

„A vasúti kiberbiztonság terén az elmúlt évek során levont tanulságok megerősítik azt a régi mondást, hogy nem lehet megvédeni azt, amit nem értesz.”

„Az erős kiberbiztonság minden digitális megoldás alapja és mozgatórugója.

Komolyan kell venni.”

[Martin Kunz;
Vezető műszaki értékesítési tanácsadó, vasúti kiberbiztonság
Siemens Mobility]

Köszönöm a figyelmet!

És további biztonságos internezetést és közlekedést kívánok! ☺

SIEMENS