Gondolatok SOC építés margójára

19 év tapasztalat után

Szabó Gábor

EIVOK 36 – SOC Tudományos konferencia

Motiváció

- Témák felvetése
- „Útjelzők” meghatározása

Tartalom

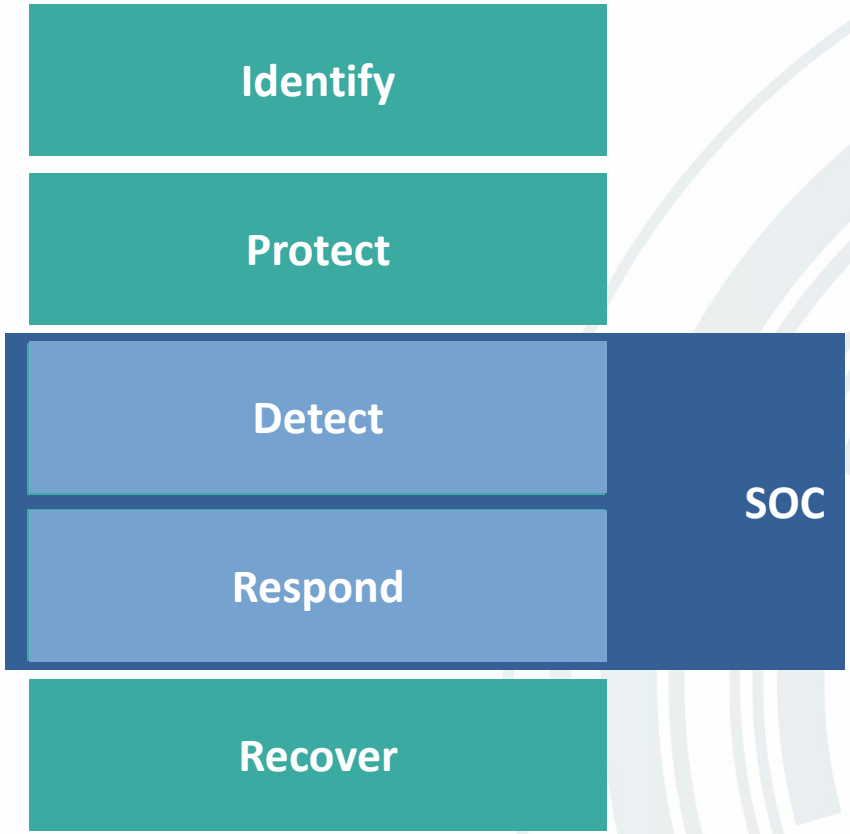
„Kell nekünk egy SOC…”

…de mit is értünk SOC alatt?

- SOC – Security Operations Center
- Évtizedes léptékben nézve a definíció („mögöttes tartalom”) változott
- „A SOC végzi a kiber incidensek kezelését!”
- „Mi a kiber incidensek kezelése, vagyis a kiber incidensmenedzsment?”
- „A kiberbiztonsági incidensek mihamarabbi észlelése és olyan válaszlépések biztosítása, amellyel minimalizálni lehet az adott incidens üzletmenetre gyakorolt hatását!”
- „Értem, de mit csinál egy CFC/CDC/SIRT/…?
- „Értem, de végül akkor a SOC üzemelteti a tűzfalakat, vagy sem?”

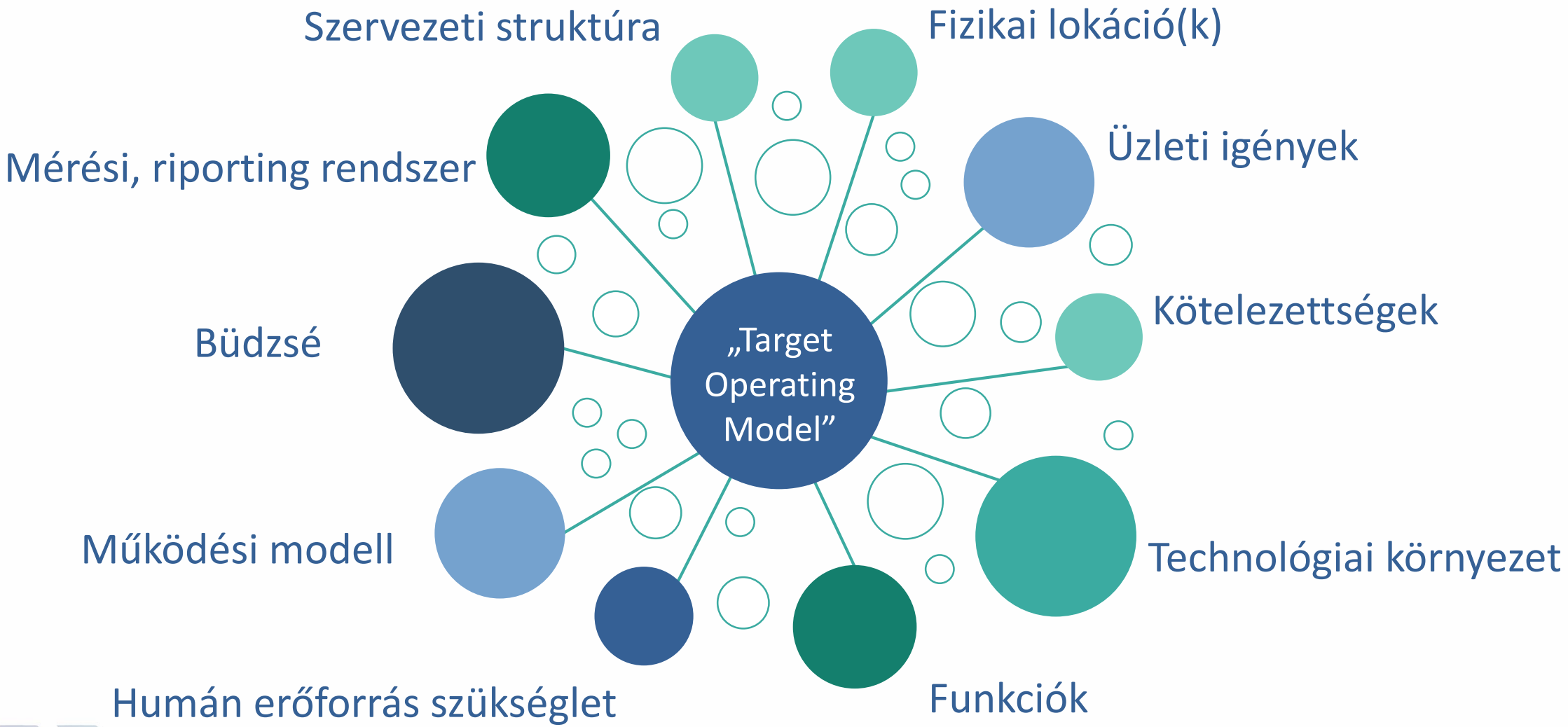
SOC, mint „képesség”

NIST CSF alapján

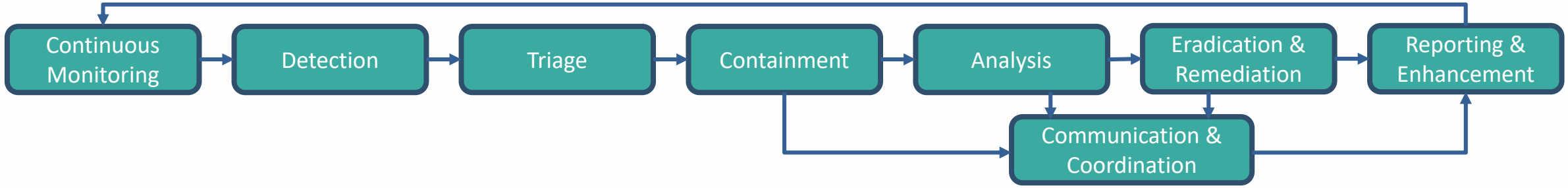


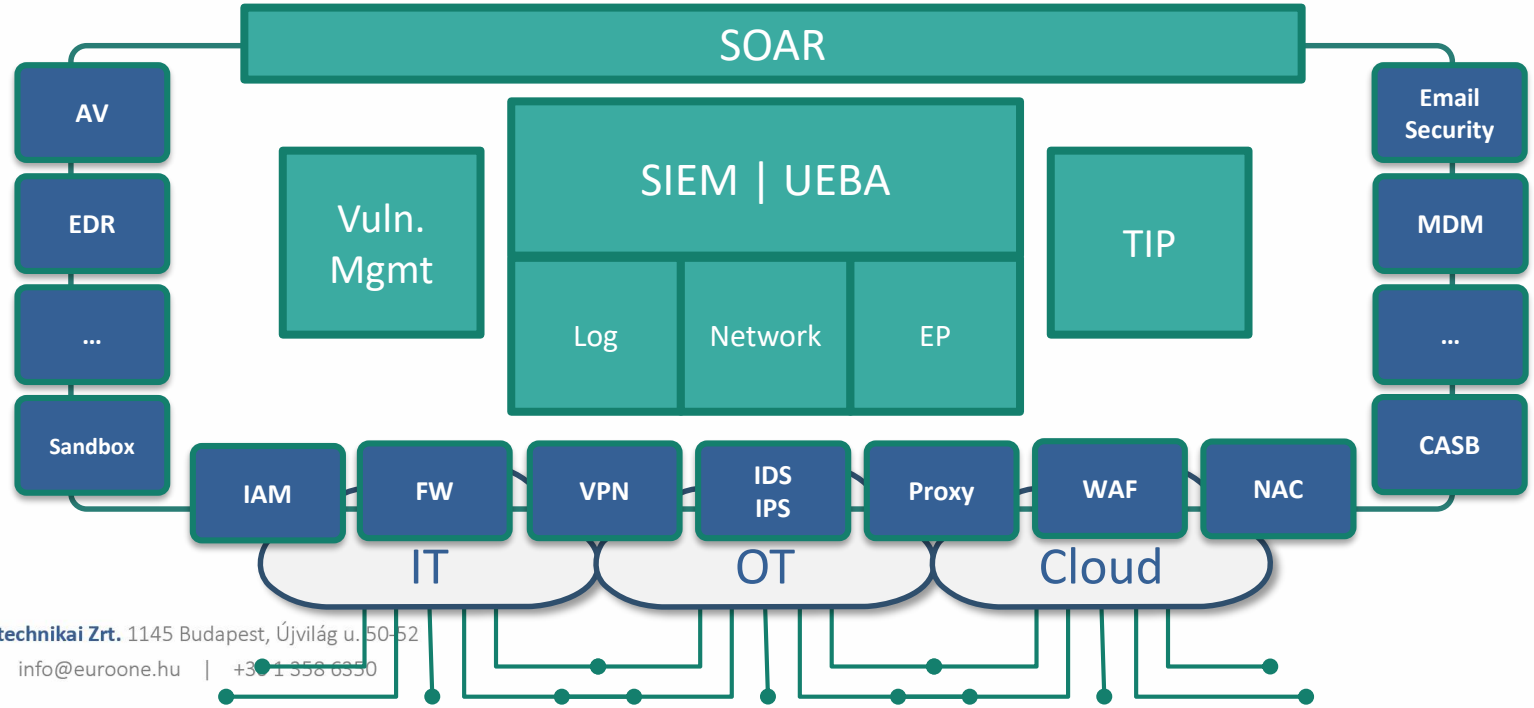
- SOC ≠ Technológia
- SOC ≠ Folyamat
- SOC = Technológia + Folyamat + Humán
- + „szervezeti kultúra”

Mit gondoljunk át?



SOC absztrakciós szintek





Hatékony SOC karakterisztikái

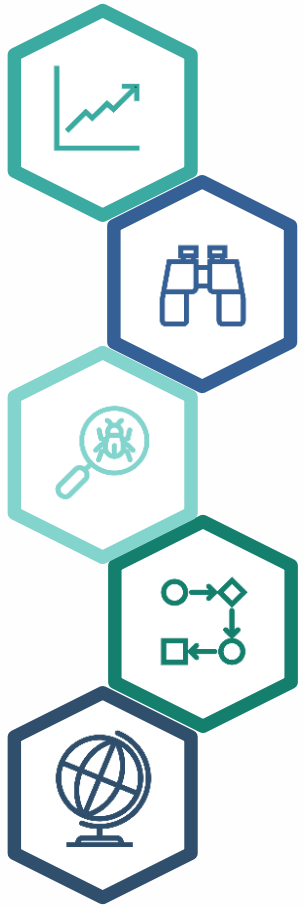
01 Üzleti igényekhez igazítás

02 „Rálátás, rálátás, rálátás!”

03 Detekciós tartalmak

04 Érett folyamatok

05 „Mi zajlik a világban?”




euro one
Köszönjük!