# Föderatív biztonsági műveleti központ létesítési tapasztalatok

Rigó Ernő <rigo@cert.hu>

HUNOG_3 2025

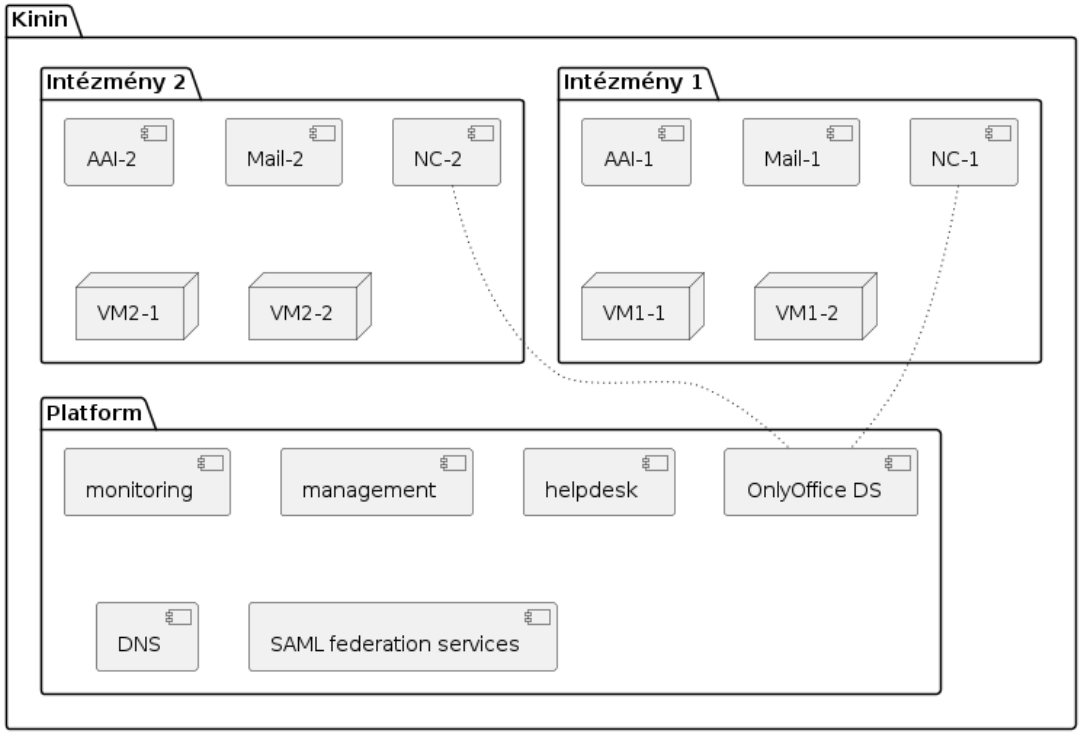
# Tartalom

- Kinin
  - Rövid áttekintés, státusz
- Kinin SOC
  - Motiváció
  - Koncepcionális áttekintés
  - Projekt ütemterv, célok, résztvevők, KPIk
  - Státusz, tervek


Kutatóhálózati Informatikai Infrastruktúra

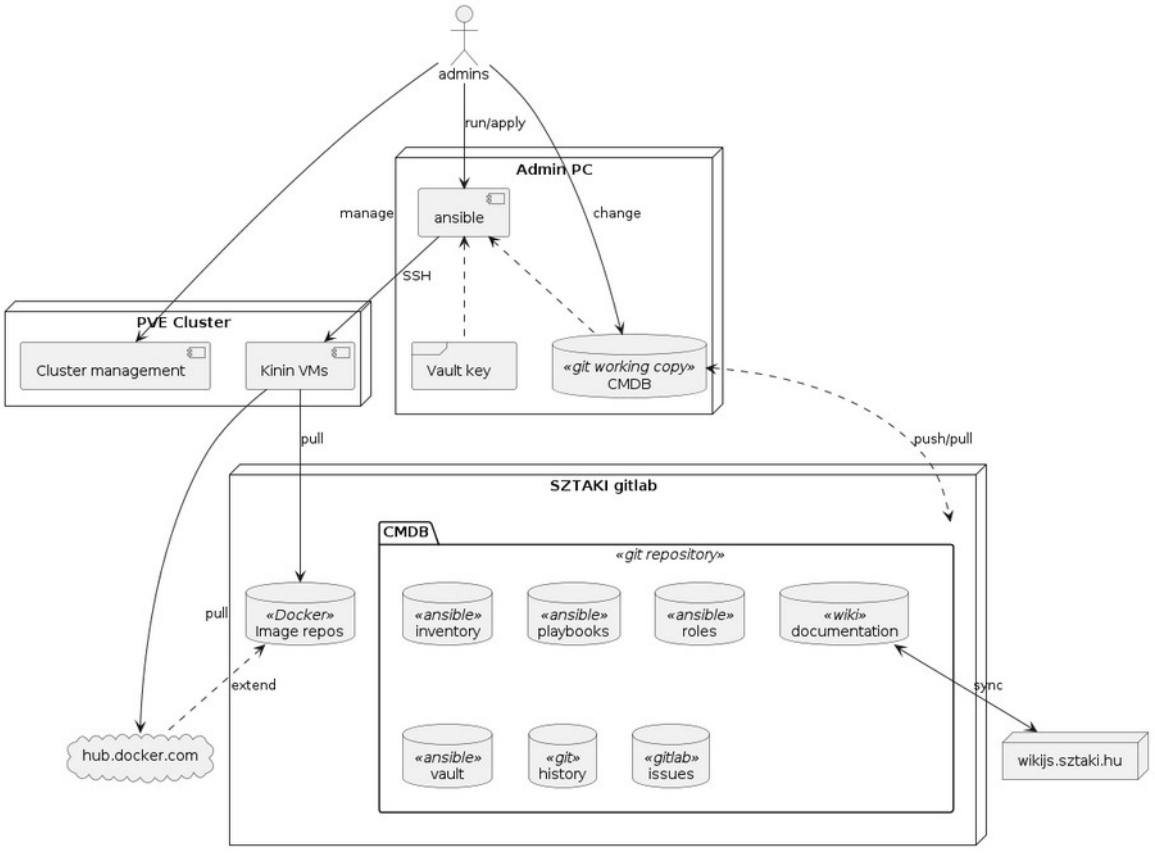
# Kinin

- Célok:
  - Wigner és SZTAKI kompetenciák közösségi hasznosítása
  - Rászoruló intézmények level 2 IT támogatása
- Modell: virtuális adatközpont
  - intézményenként dedikált szolgáltatások
  - közös szolgáltatási sablonok



# Kinin menedzselt szolgáltatások

- AAI
  - felhasználó- és csoportmenedzsment (LDAP, Radius, SAML)
- Mail
  - korszerű levelezési környezet (SMTP, IMAP, Webmail)
- NC
  - tárhely és csoportmunka (Nextcloud)
- VM
  - Linux vagy Windows VM
- Matrix
  - Instant messaging

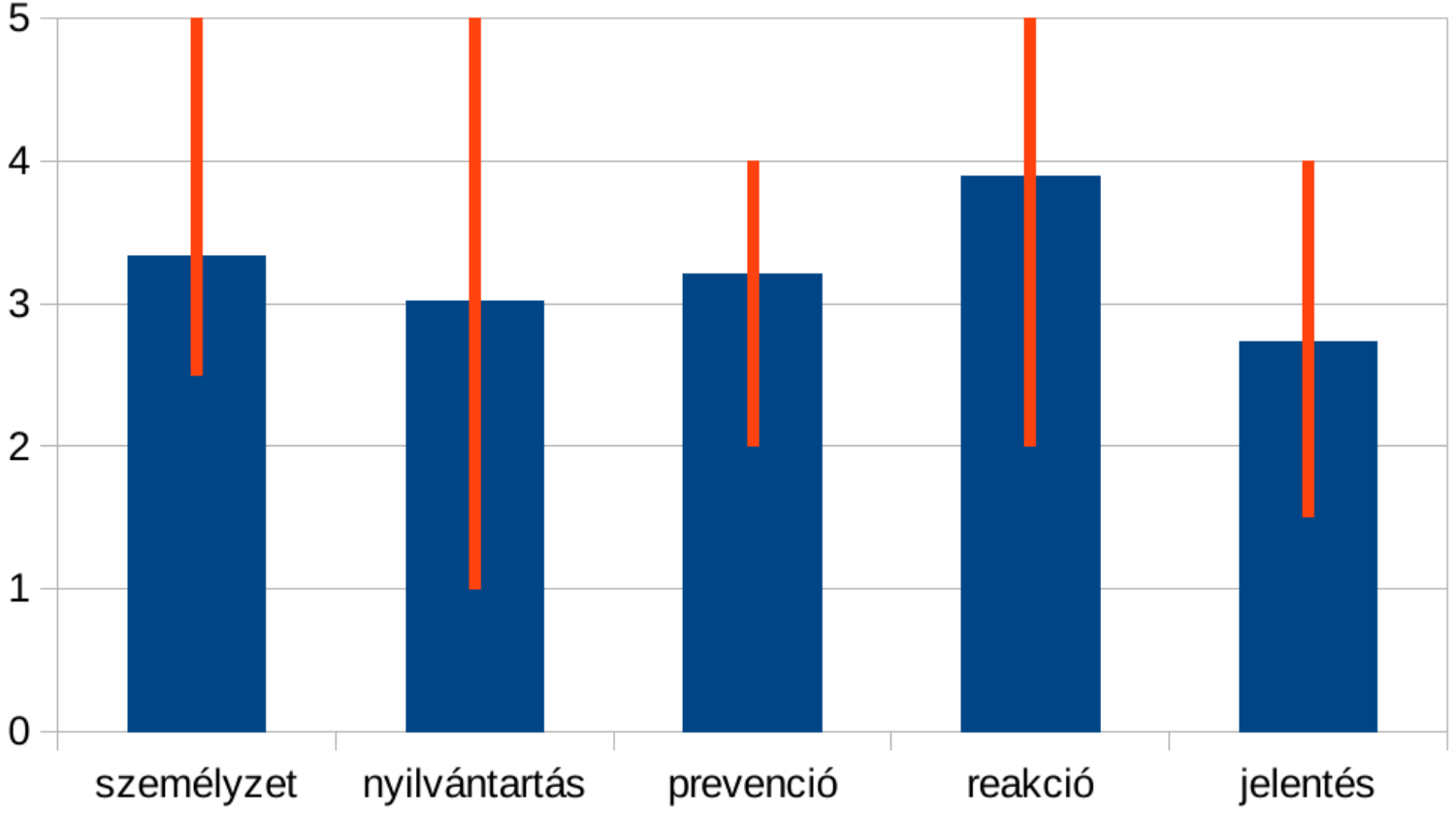


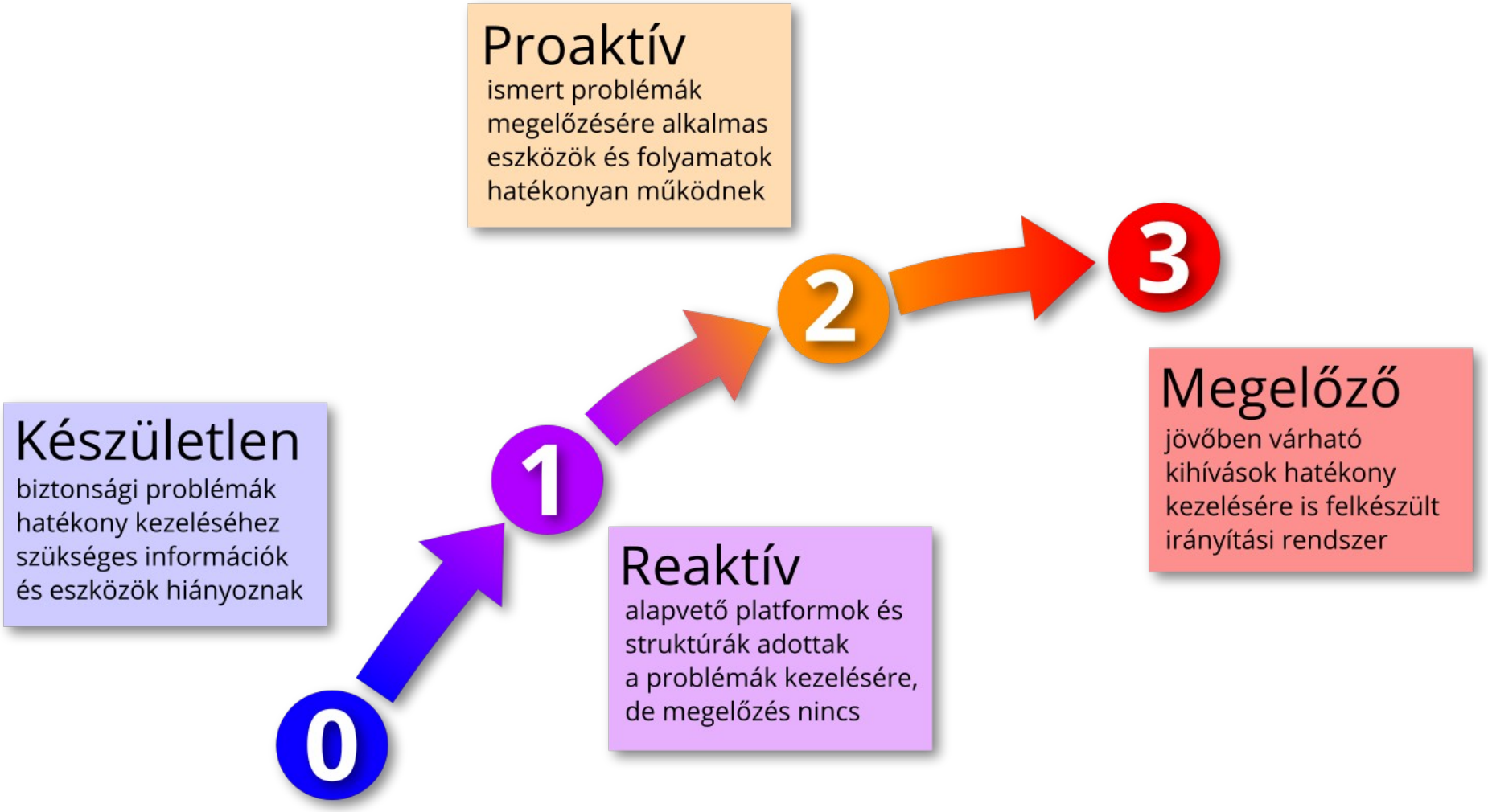
Kinin SOC

# Projekt motiváció

- Kutatóhálózat
  - Külső elvárások
    - IBTV hatókör változások
    - NIS2, SZTFH
  - Kitettség
    - Nemzeti (adat)vagyon
    - Növekvő incidensszám
  - Belső elvárások
    - Információbiztonsági keretszabályzat
- HUN-REN SZTAKI
  - Beágyazottság, kompetencia
    - HunCERT
    - Kinin
    - HUN-REN Cloud / ARP
  - Külső finanszírozási lehetőség
    - SOCCER
      - DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs)
      - 3 év, 50%-os támogatási intenzitás
  - Felmérési eredmények
    - Egybevágó kutatóhelyi igények
    - Sérülékenységvizsgálat eredményei

# Igényfelmérés - önértékelés (2023)



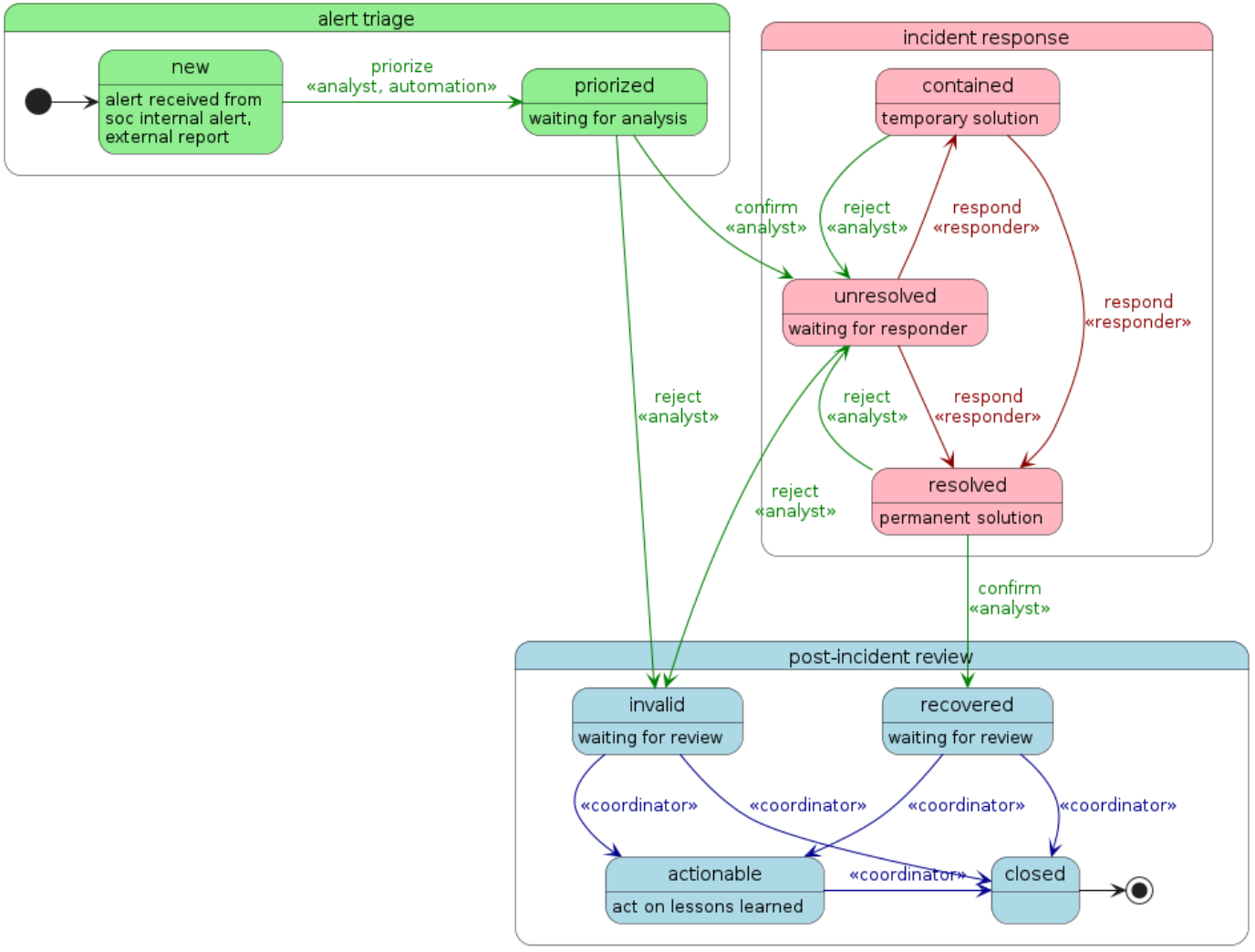

Proaktív
ismert problémák
megelőzésére alkalmas
eszközök és folyamatok
hatékonyan működnek
Készületlen
biztonsági problémák
hatékony kezeléséhez
szükséges információk
és eszközök hiányoznak
Reaktív
alapvető platformok és
struktúrák adottak
a problémák kezelésére,
de megelőzés nincs
Megelőző
jövőben várható
kihívások hatékony
kezelésére is felkészült
irányítási rendszer
0
1
2
3

# Biztonságmenedzsment

- Proaktív
  - Cél: eső előtt köpönyeg
  - Eszközei:
    - Sérülékenységvizsgálat
    - Penetrációs tesztek
    - Kibervédelmi gyakorlatok
    - Oktatás és képzés
    - Hír- és trendfigyelés
    - Fenyegetésvadászat (Threat Hunting)
    - CTI (Cyber Threat Intelligence) megosztása, feldolgozása
- Reaktív
  - Cél: károk minimalizálása
  - Eszközei:
    - Incidens észlelés
      - IoC (Indicators of Compromise)
      - Folyamatos monitoring
      - Naplóelemzés
      - Threat Hunting
    - Incidensmenedzsment
      - (lásd: következő dia)
- Mindkét megközelítés szükséges!

# Incidensmenedzsment

- Elemzés (alert triage)
  - Riasztások forrása:
    - Manuális vagy automatikus
  - Lépései:
    - Priorizálás
      - Sok riasztás nem riasztás
      - Nehéz feladat!
    - Kontextualizáció
      - Tudásbázis, naplóelemzés
      - Vagyonleltár, historikus adatok, CTI
    - Eszkaláció
      - Fals pozitív vagy incidens?
- Incidens kezelése
  - Körülhatárolás (containment)
    - hálózati forgalom korlátozása
    - processzek leállítása
    - jelszócsere
  - Megoldás (eradication)
    - sérülékenység javítása
    - konfiguráció módosítás
  - Helyreállás (recovery)
    - intenzív megfigyelés
- Incidens utáni értékelés
  - Új automata riasztások, forgatókönyvek
  - Folyamatok finomítása, dokumentáció


alert triage
new
alert received from soc internal alert, external report
priorize
«analyst, automation»
priorized
waiting for analysis
incident response
contained
temporary solution
confirm
«analyst»
reject
«analyst»
respond
«responder»
unresolved
waiting for responder
respond
«responder»
reject
«analyst»
respond
«responder»
reject
«analyst»
resolved
permanent solution
reject
«analyst»
confirm
«analyst»
post-incident review
invalid
waiting for review
recovered
waiting for review
«coordinator»
«coordinator»
«coordinator»
«coordinator»
actionable
act on lessons learned
«coordinator»
closed

# Projekt célok

- Föderatív biztonsági műveleti központ létrehozása
  - Föderatív információmegosztás
    - Adatcsere felület
    - Folyamatok
  - Reaktív szolgáltatások:
    - Központi biztonsági kompetencia, elemző és támogató szolgáltatások
    - Incidens koordináció
  - Proaktív szolgáltatások:
    - Önálló információgyűjtés
      - Csapdarendszer
      - Biztonsági pásztázások
      - Biztonsági hírfolyamok
- Helyi mintamegoldások biztosítása
  - Naplógyűjtés- és elemzés
  - IT vagyonelem leltár
  - Sérülékenységvizsgálat
- Szelektív adattovábbítás
  - Helyi → központi
    - Vagyonelem típusok
    - Biztonsági esemény naplók
  - Központi → helyi
    - Riasztások, incidensek
    - Használati minták
  - Központi → külvilág
    - Trendek, események

# KPIk

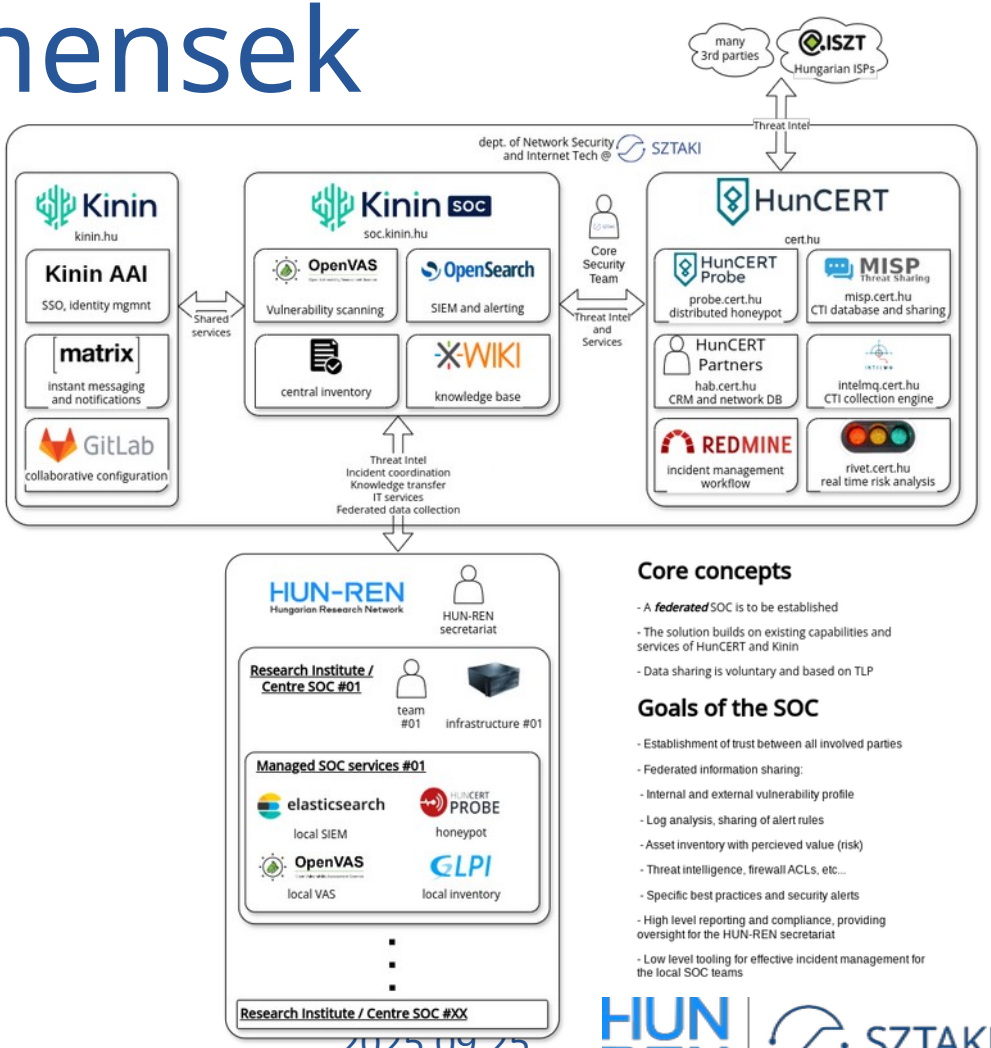
- Központ
  - 4db éles üzembe kerülő új központi SOC szolgáltatási elem
  - 4db átadásra kerülő kutatóhelyi SOC szolgáltatási elem
  - Projekt eredményeit bemutató oktatás és workshop
  - Biztonsági gyakorlat eredményét bemutató jelentés
- Kutatóhelyek
  - Részvétel a projekt az oktatáson és workshopon
  - Értékelhető részvétel a biztonsági gyakorlaton
  - Legalább 1db kutatóhelyi SOC szolgáltatási elem üzembe állítása

# Adatmegosztás

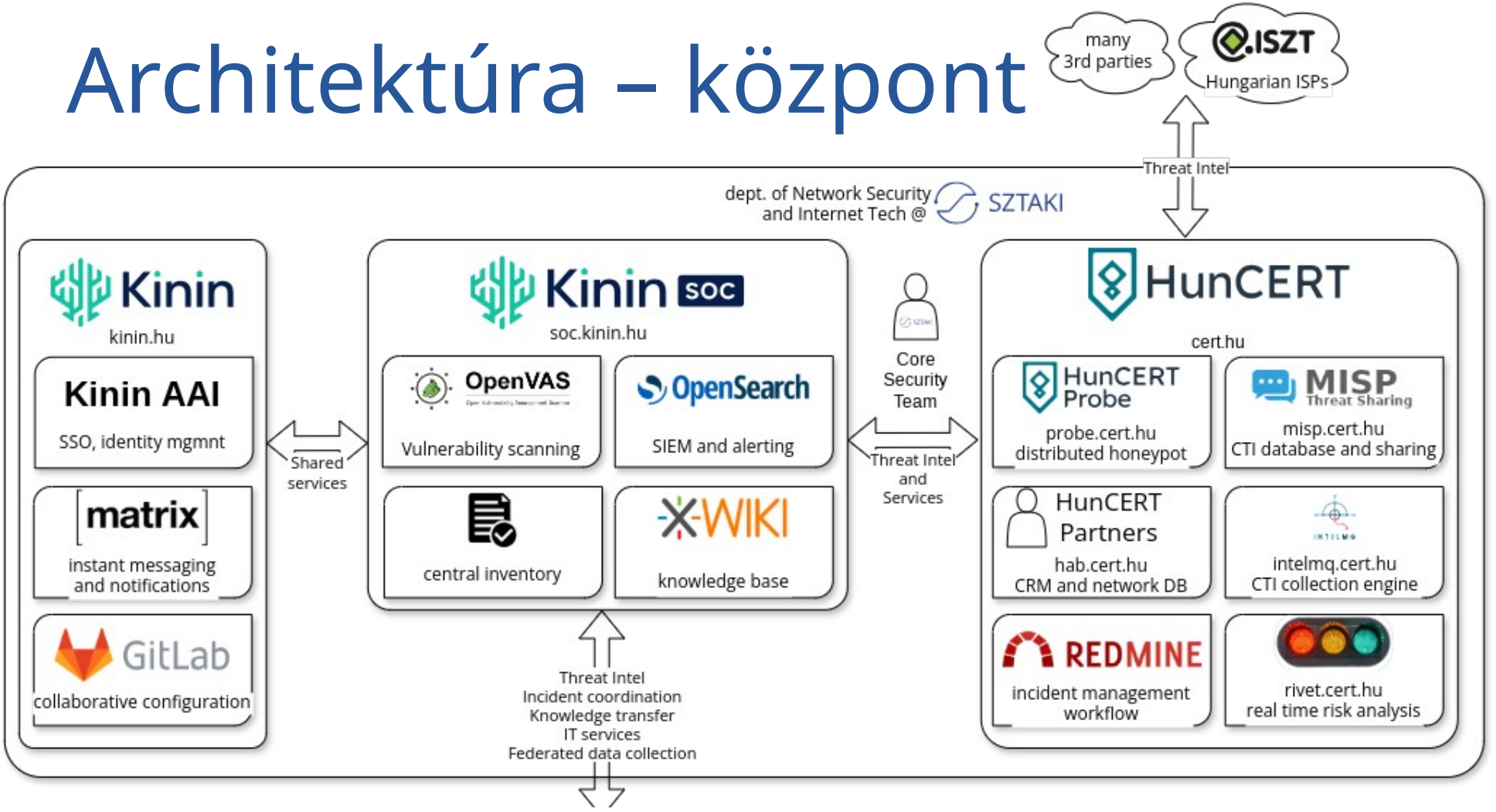
- Alapelvek
  - Célhoz kötöttség
    - A központ nem gyűjt feleslegesen adatot
    - Nem osztunk meg feleslegesen adatot külső felek számára sem
  - Önrendelkezés
    - A kibocsátott adatok címkézése
    - Alapérték: TLP:AMBER
  - Átláthatóság
    - A központban tárolt adatok hozzáférhetők, ellenőrizhetők
    - Különösen: SIEM, Inventory, KB
- TLP (Traffic Light Protocol)
  - ⚪ TLP:CLEAR (korábban: WHITE)
    - Nyilvános információk
  - 🟢 TLP:GREEN
    - HUN-REN közösség számára
    - Egyes azonosítók maszkolva
  - 🟠 TLP:AMBER
    - Csak a központ és az adott intézmény számára
  - 🔴 TLP:RED
    - Csak személyes használatra (ritka)

# Komponensek

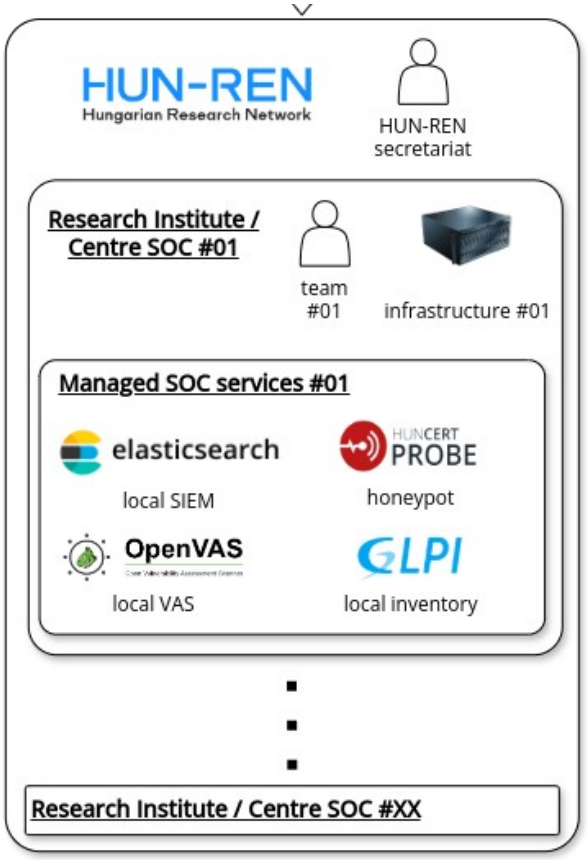
- Infra – alapinfrastruktúra
- Probe – csapdarendszer
- SIEM – naplóelemzés és riasztások
- TI – threat intel, adatcsere
- Ticketing – folyamattámogatás
- VAS – sérülékenységvizsgálat
- Inventory – leltár
- KB – tudásbázis



# Architektúra – központ



# Architektúra – intézmények




## Core concepts

- A ***federated*** SOC is to be established

- The solution builds on existing capabilities and services of HunCERT and Kinin

- Data sharing is voluntary and based on TLP

## Goals of the SOC

- Establishment of trust between all involved parties

- Federated information sharing:

- Internal and external vulnerability profile

- Log analysis, sharing of alert rules

- Asset inventory with percieved value (risk)

- Threat intelligence, firewall ACLs, etc...

- Specific best practices and security alerts

- High level reporting and compliance, providing oversight for the HUN-REN secretariat

- Low level tooling for effective incident management for the local SOC teams

# SOC szerepkörök

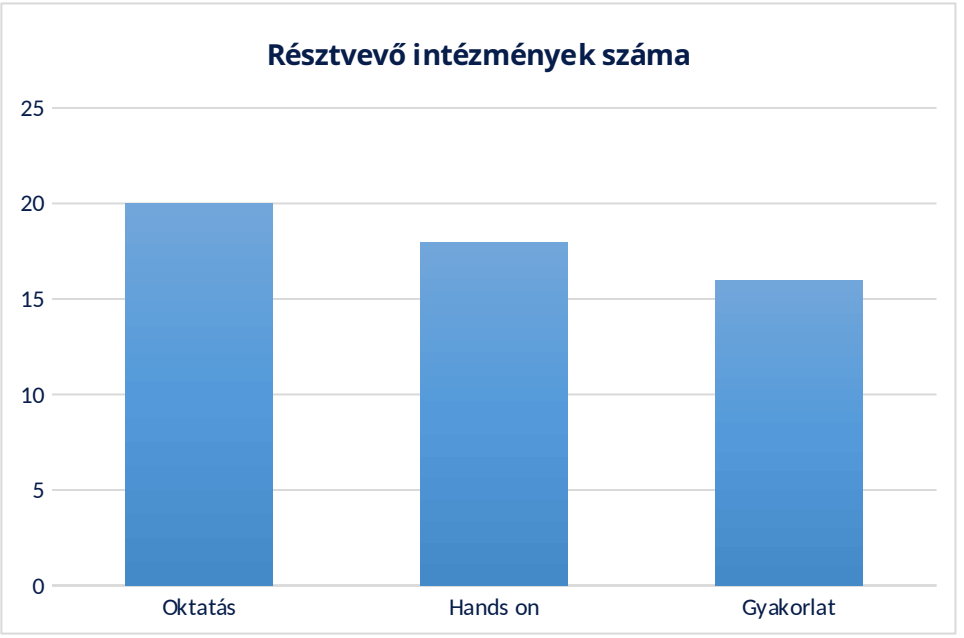
- Coordinator (K - központi)
  - Folyamatirányítás
  - Jelentések
  - Tudásmenedzsment
- Analyst / elemző (K)
  - Elsődleges (L1) és másodvonal (L2)
  - Riasztások elemzése
  - Kontextus összegyűjtése
- Threat hunter (K)
  - Proaktív adatelemzés
  - Riasztások
- Incident responder (H - helyi)
  - Hatás csökkentése
  - Kárelhatárolás
  - Végleges megoldás
- Engineer / mérnök (K, H)
  - Műszaki beavatkozások
  - Telepítés, konfiguráció
- Manager (K)
  - Szabályzati megfelelőség
  - Szerepkörök koordinációja

# Státusz

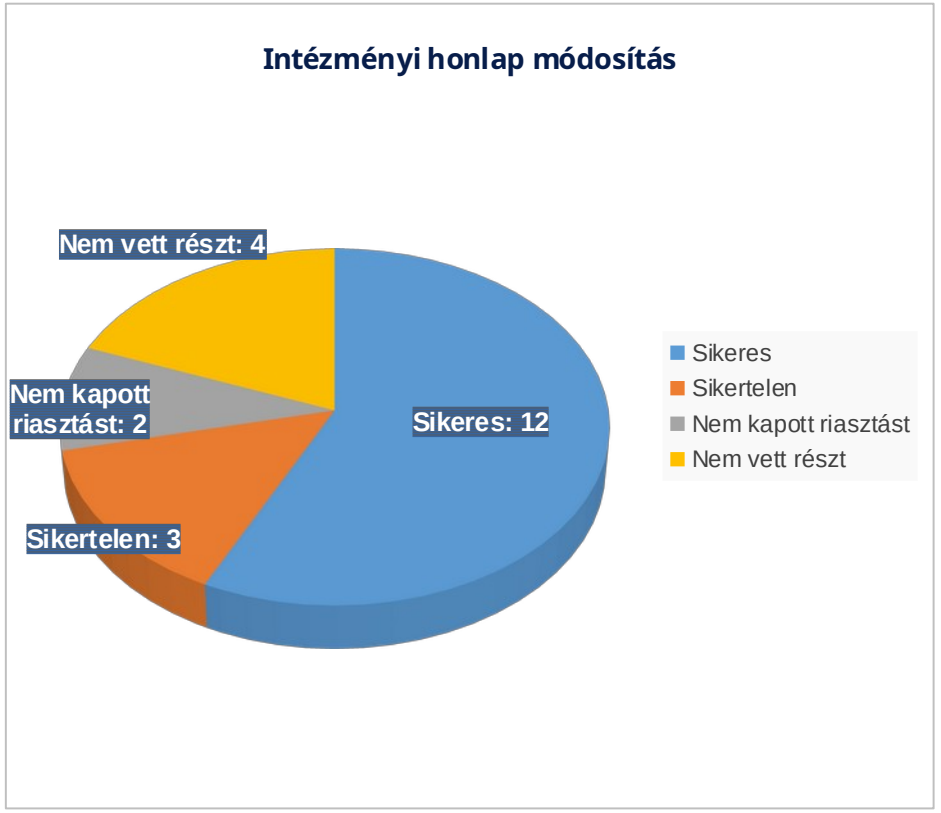
- A projekt számokban: 20 meghívott intézmény, 3 workshop, 17 SZTAKI HBIT munkatárs, 3.5+ emberév, 110 db magasszintű létesítési feladat, 330 oldal rendszerterv, 250 oldal felhasználói dokumentáció, 41 db GitLab repozitórium
- Egyéb hozadékok
  - Phishing teszt szolgáltatás
  - Biztonság tudatossági oktatóanyag
  - Hands-on tapasztalatok

# Bevezető gyakorlat

- 2025. március 24.
- Feladatok
  - 1. kommunikáció, incident response (sérülékeny weblap javítása)
  - 2. specifikus műszaki feladat (tűzfal konfiguráció)
- Aktív részvétel: 76%
  - Kitelepített SIEM vagy Probe appliance: 75%



# 1. feladat (webes sérülékenység)




- Első reakció:
  - 60 percen belüli visszajelzési arány: 68%
  - 24 órás küszöbértéken túl: 1 intézmény
- Megoldás:
  - 60 percen belül: 42%
  - sikertelen: 3 intézmény

# 2. feladat (tűzfal konfiguráció)

# Tervek

- Bevezetési, működési szakasz
  - Központi KPIk
    - K1.1 Külső forrásból származó, feldolgozott biztonsági események száma
    - K1.2 Hatáskörben észlelt és kezelt biztonsági események száma
    - K1.3 Kibocsátott általános riasztások és tájékoztatások száma
    - K1.4 Kibocsátott célzott információs jelentések (TI, vulnerability report) száma
    - K1.5 Biztonsági gyakorlatról készült és egyéb értékelő jelentések száma
  - Intézményi KPIk
    - K2.1 Központ számára megosztott biztonsági események száma
    - K2.2 Központ számára megosztott vagy aktualizált biztonsági profil elemek száma
    - K2.3 Központi biztonsági analízis számára megosztott adatforrások száma
    - K2.4 Központ számára megosztott biztonsági információk (TI) száma
    - K2.5 Biztonsági gyakorlaton történő részvételek száma

- Folytamatos fejlődés, visszacsatolás, finomhangolás
- További tervezett fejlesztések
  - CTI korreláció alapú érzékelés (továbbfejlesztése)
  - Playbookok, automatizált reakciók (pl. n8n)
  - AI-driven funkciók
  - XDR (pl. Elastic Endpoint)
  - Üzleti támogató komponensek (pl. Elastic, QRadar, XSOAR)

# Kinin SOC finanszírozás

- DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs)
  - 504 505 €, melyből 252 252 € önerő
  - Trout Software (FR/IR)
  - Signal Iduna (DE)
  - Orange Romania (RO)
- Létesítési projekt:
  - HUN-REN támogatás

# Köszönöm a figyelmet!