HUNCERT

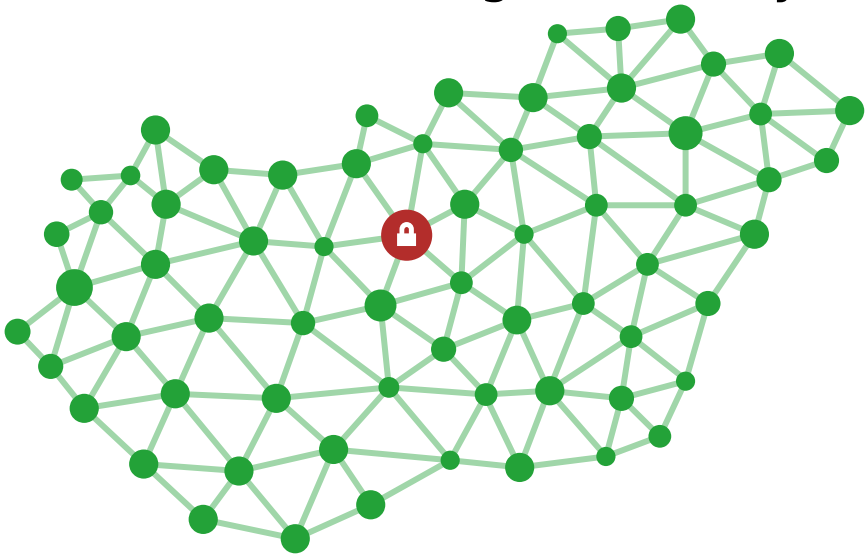
Incidenskezelési Gyakorlat

Towel Day 2021 – On-line, 2021.05.25.

Rigó Ernő <rigo@cert.hu>

ISZT HunCERT

- Alapító és támogató:
  - Internet Szolgáltatók Tanácsa (nonprofit egyesület)
  - SZTAKI (nonprofit, az Eötvös Loránd Kutatóhálózat tagja)
- Üzemeltető: SZTAKI Hálózatbiztonsági és Internet Technológiák Osztálya
- Alapítva: 2003 október
- Tevékenységek, szolgáltatások
  - Hálózatbiztonsági incidensek kezelése
  - Biztonsági tudatosság növelése
  - Publikációk, oktatás, hírek, riasztások
  - Koordináció
  - Hálózatbiztonsági eszközfejlesztés



Kommunikációs gyakorlat

- Célok:
  - Együttműködés javítása
  - Kapcsolati adatok frissítése
  - Készenlét ellenőrzése
- Meghívott résztvevők:
  - ISZT tagok: 44 darab
  - BIX tagok: 78 darab
  - Domain Regisztrátorok: 136 darab
- A részvétel önkéntes

Előkészítés

- Tervezés
  - Téma meghatározása
  - Előkészítési feladatok listája
  - Forgatókönyv megtervezése
    - Kommunikáció ütemezése, pontos tartalma
  - Utóhatások, záró feladatok
- Monitoring rendszer előkészítése
- Résztvevő lista összeállítása
- Engedélyek megkérése

A gyakorlat témája és forgatókönyve

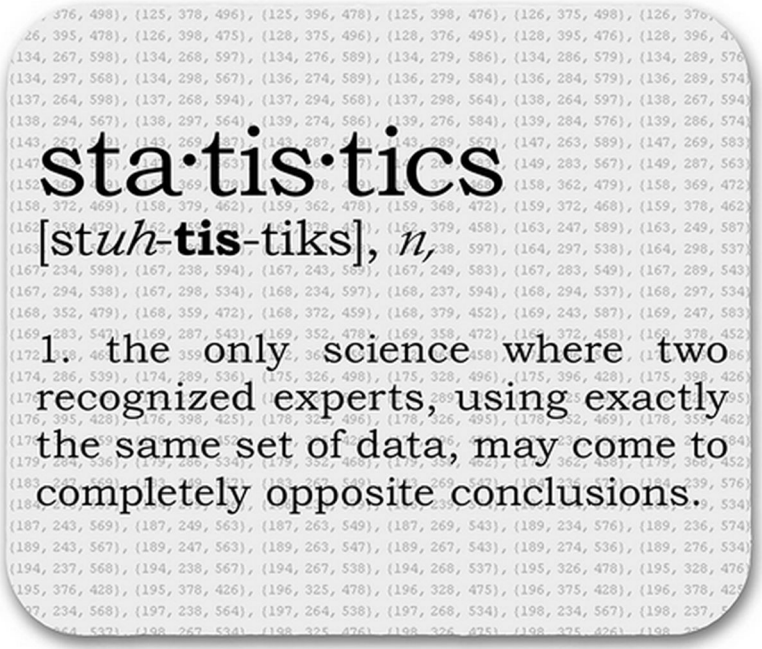
- Feltételezett DDoS kampány központi DNS szerverek ellen
- Forgatókönyv
  - 1. levél:
    - gyakorlat indítása
    - kapcsolati adatok frissítése (hab.cert.hu)
    - IDS/IPS log elemzés (vagy: PROBE log elemzés)
  - megismételt 1. levél
    - kb. 3 nap múlva a passzív résztvevők számára
  - 2. levél:
    - gyakorlat zárás

Utómunka, zárás

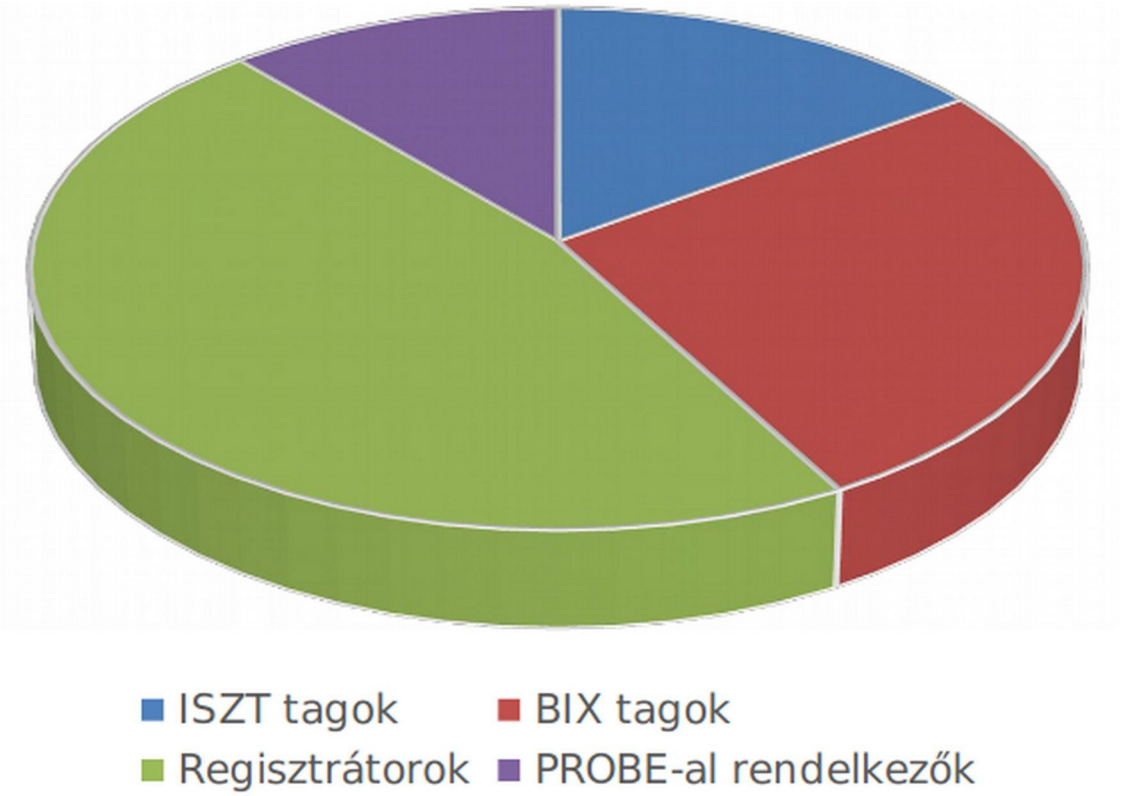
- Problémák közvetlen feltárása
- Monitoring leállítása
- Eredmények elemzése
- Tanulságok értékelése
- Értékelő jelentés publikálása
- Vezetői összefoglaló
- Beszámolók tartása
- Következő gyakorlat előkészítése

Eredmények

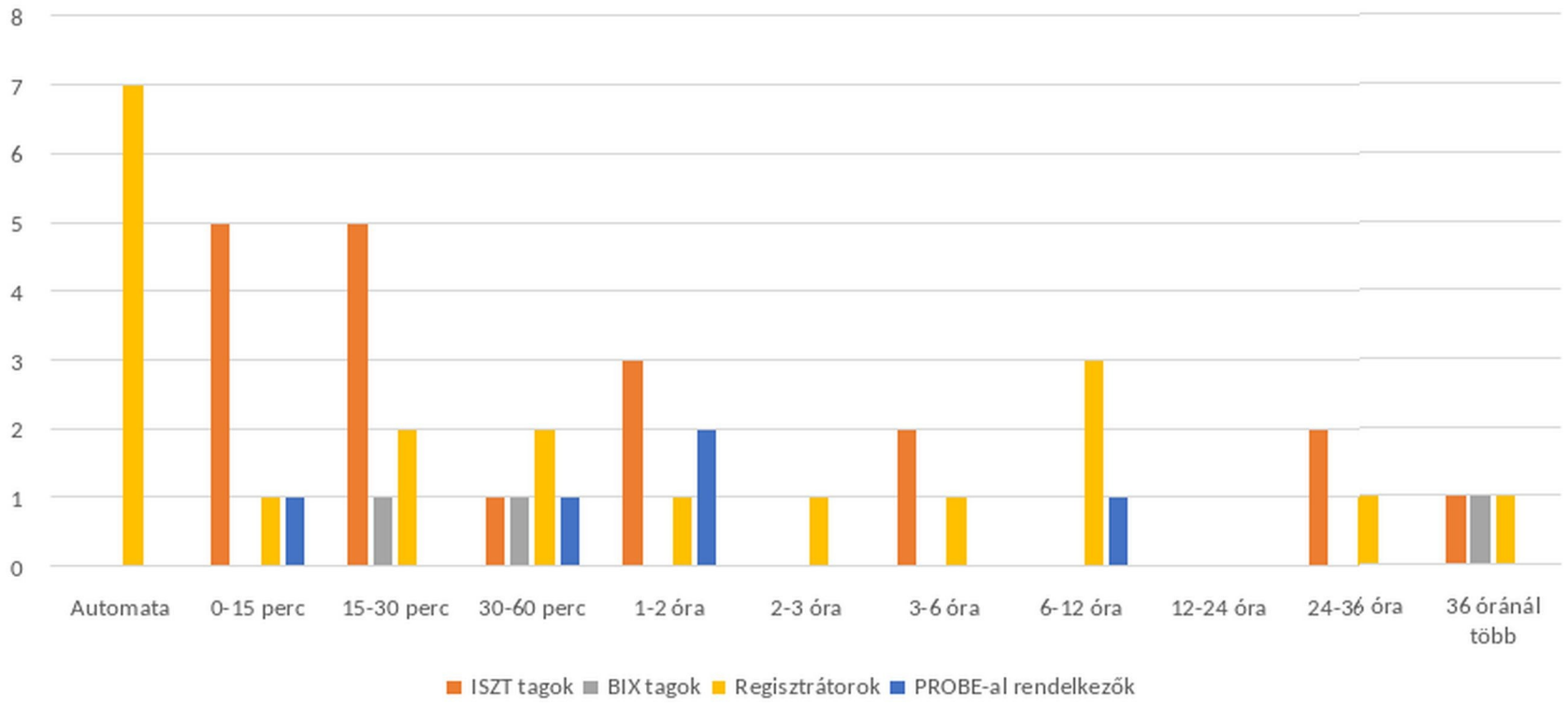
- Résztvevők
  - ISZT / BIX tagok: 19 darab
  - Regisztrátorok: 32 darab
- Válaszlevél: 44 darab
- Medián válaszidő: 15-30 perc
- Többen csak a nyitó levélre válaszoltak
- Részvétel viszonylag alacsony



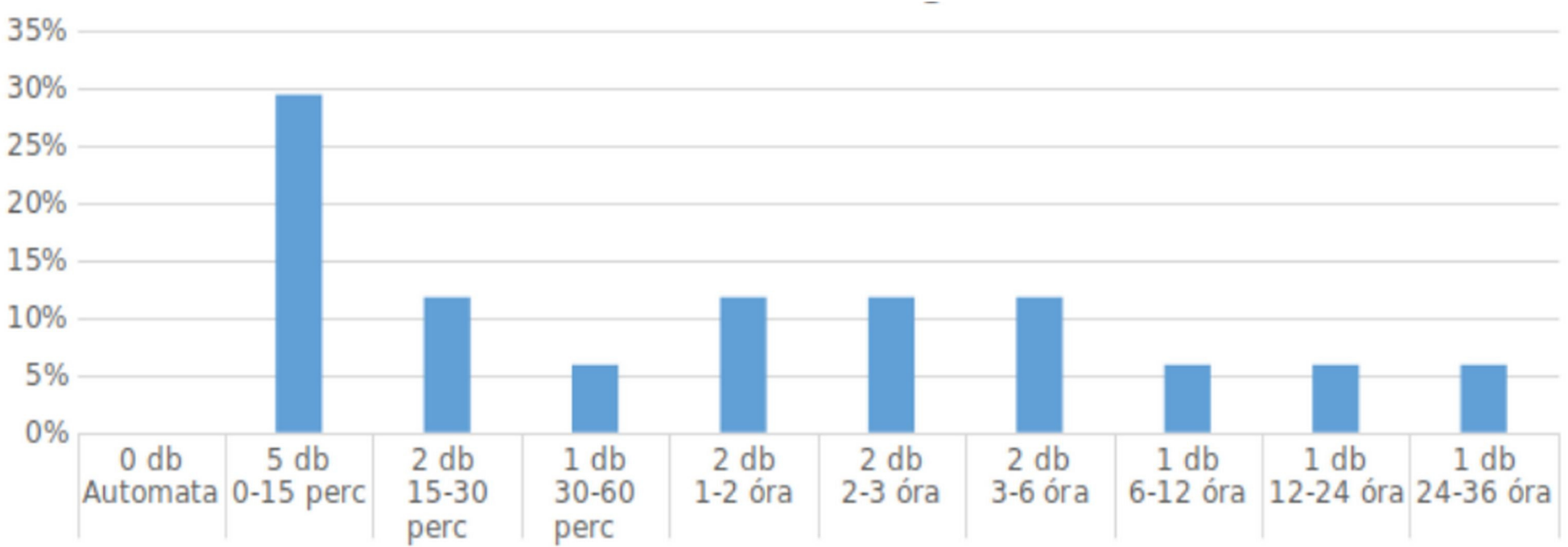
Résztvevők megoszlása



Reakcióidők – nyitó levél



Reakcióidők – záró levél



Kérdések?

Köszönjük a figyelmet!

http://www.cert.hu
cert@cert.hu