NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
NEMZETI KIBERVÉDELMI INTÉZET

Csapdarendszerek

2020.05.20
Budapest

NEMZETI KIBERVÉDELMI INTÉZET

Marsi Tamás

Ügyfelek

NKI

2013. L tv.
Állami szervezetek
Önkormányzatok

NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

- Egyéb szervezetek
- Oktatási intézmények
- NB védelem alá eső szervezetek

2009/2015 korm. hat.

- Közvetítő szolgáltató

Megfelelőség (hatóság)
Incidenskezelés
Sérülékenységvizsgálat

2012. CLXVI. tv 2/A §
- Energia
- Közlekedés
- Agrárgazdaság
- Egészségügy
- Társadalombiztosítás
- Pénzügy
- Infokommunikációs technológiák
- Vízgazdálkodás
- Közbiztonság-védelem
- Honvédelem (HÁEIBEK)

2001. CVIII. tv 2 § j)
- Online piactér
- Keresőszolgáltatás
- Felhőalapú szolgáltatás

- Nemzeti létfontosságú szolgáltató

271/2018 korm. rend.
Bejelentés köteles szolgáltató
- Egyszerű adatszolgáltatással érintett
- Gyorsítótárazás
- Keresőszolgáltatás

Nemzeti Kibervédelmi Intézet

NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

- Incidens-kezelés
- L1
- L2
- Riasztás
- Tájékoz-tatás

- L3
- Log-elemzés
- Forensics
- Malware elemzés

- EWS
- Honeypot
- Big data

- Külső
- Belső
- Webes
- Wifi
- Social engineer-ing

- Biztonság-irányítás
- Biztonság-felügyelet

- Nyilván-tartás
- Ellenőrzés
- SPOC
- Tudatos-ítás

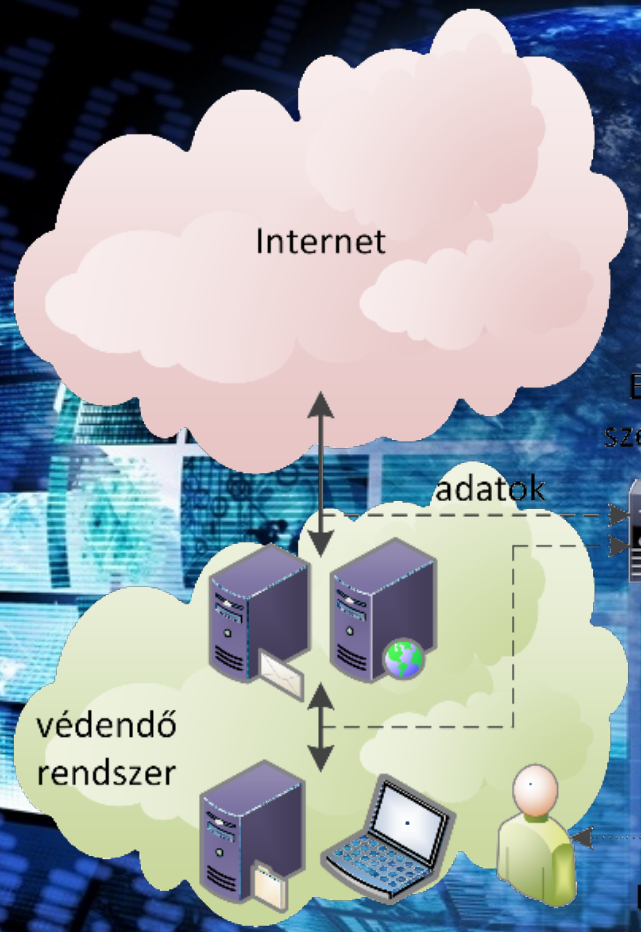
Rendszerek

EWS

Honeypot (GovProbe)

Big Data (Biléta)

EWS



EWS – adatgyűjtés

szolgáltatás nyújtása

NKI és védett intézmény részére

Csatlakozás műszaki követelményei

hálózati forgalom átadása

titkosítás feloldása

kritikus hálózati csomópontok kialakítása

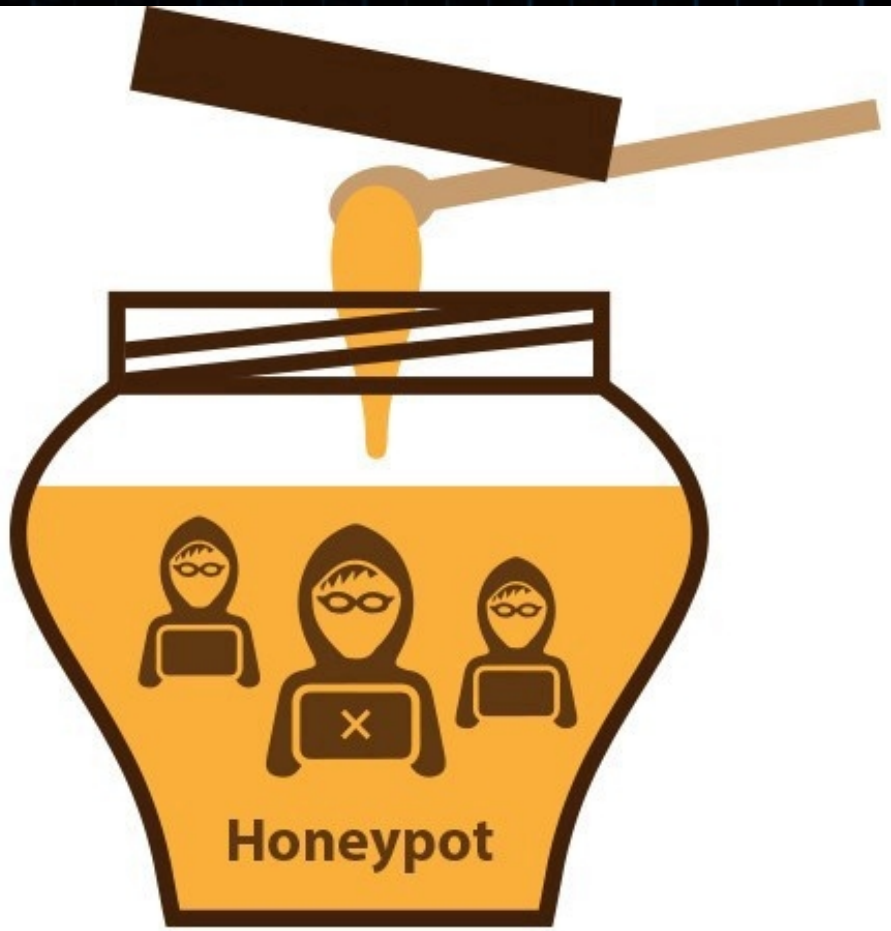
naplókezelési minimumkövetelmények

Biléta - infrastruktúra

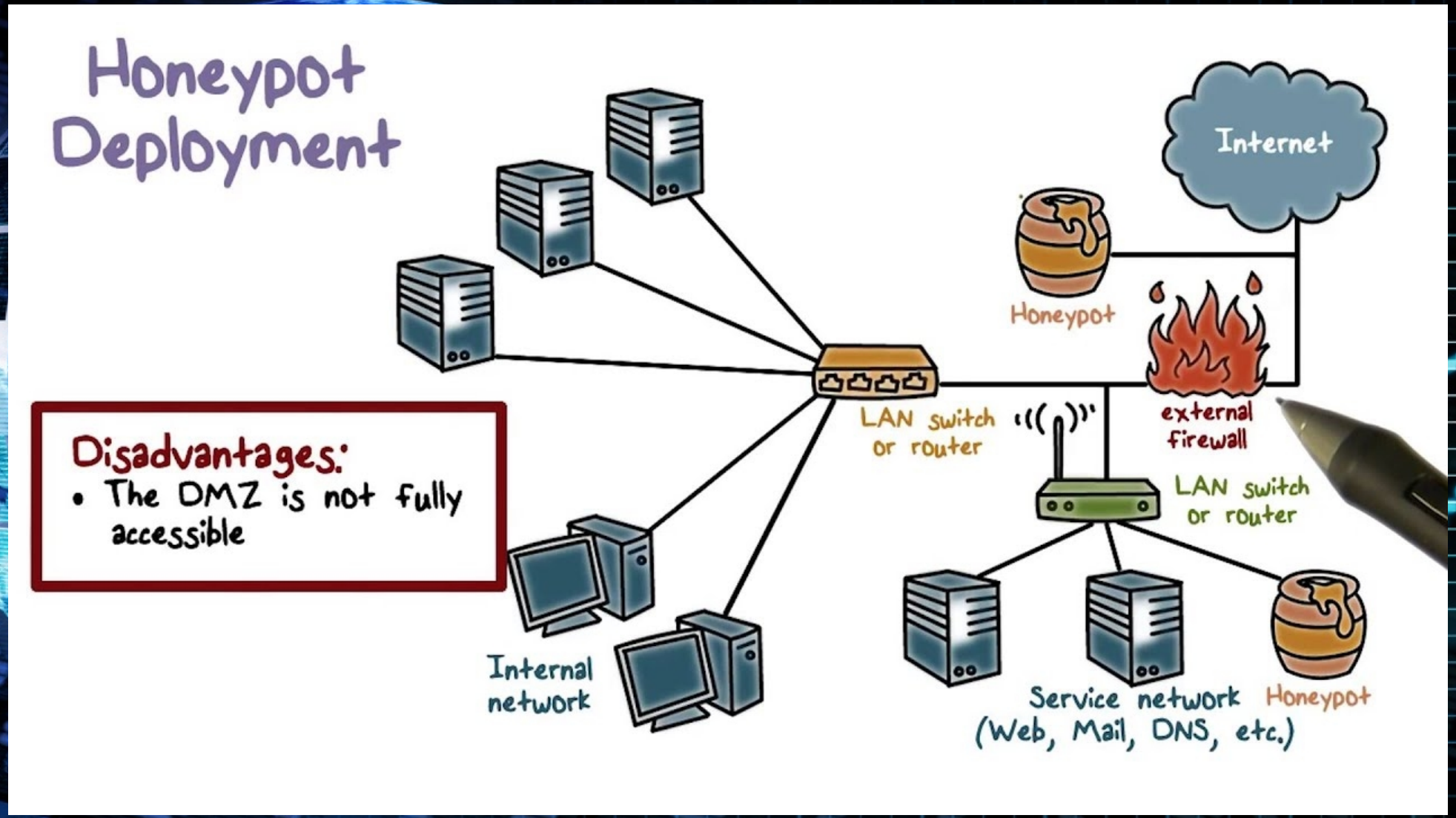
- Hadoop alapú adattárolási rendszer
  - Cloudera Impala
  - Impala queries
  - Impala interfész
  - Flume agent

HONEYPOT

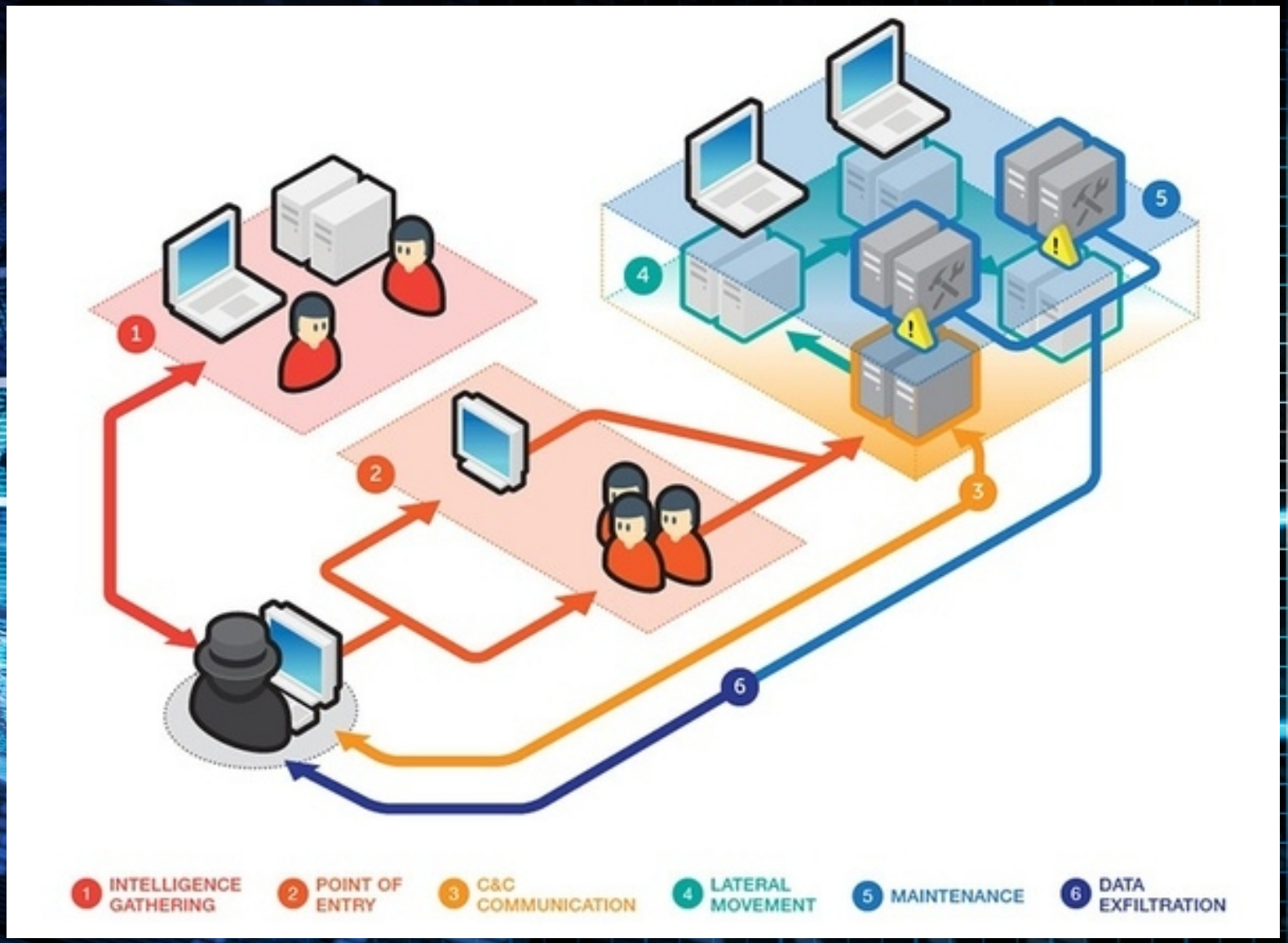
Honeypot



Elhelyezés


Honeypot Deployment
Internet
Honeypot
external firewall
LAN switch or router
LAN switch or router
Disadvantages:
• The DMZ is not fully accessible
Internal network
Service network (Web, Mail, DNS, etc.)
Honeypot

Honeypot és APT



Honeypot

a támadó tevékenységét összegyűjti, rögzíti, naplózza

a támadó saját magát leplezi le

valós működést szimuláló, álcázott szolgáltatások:

tűzfal

SSH

ARP, DHCP

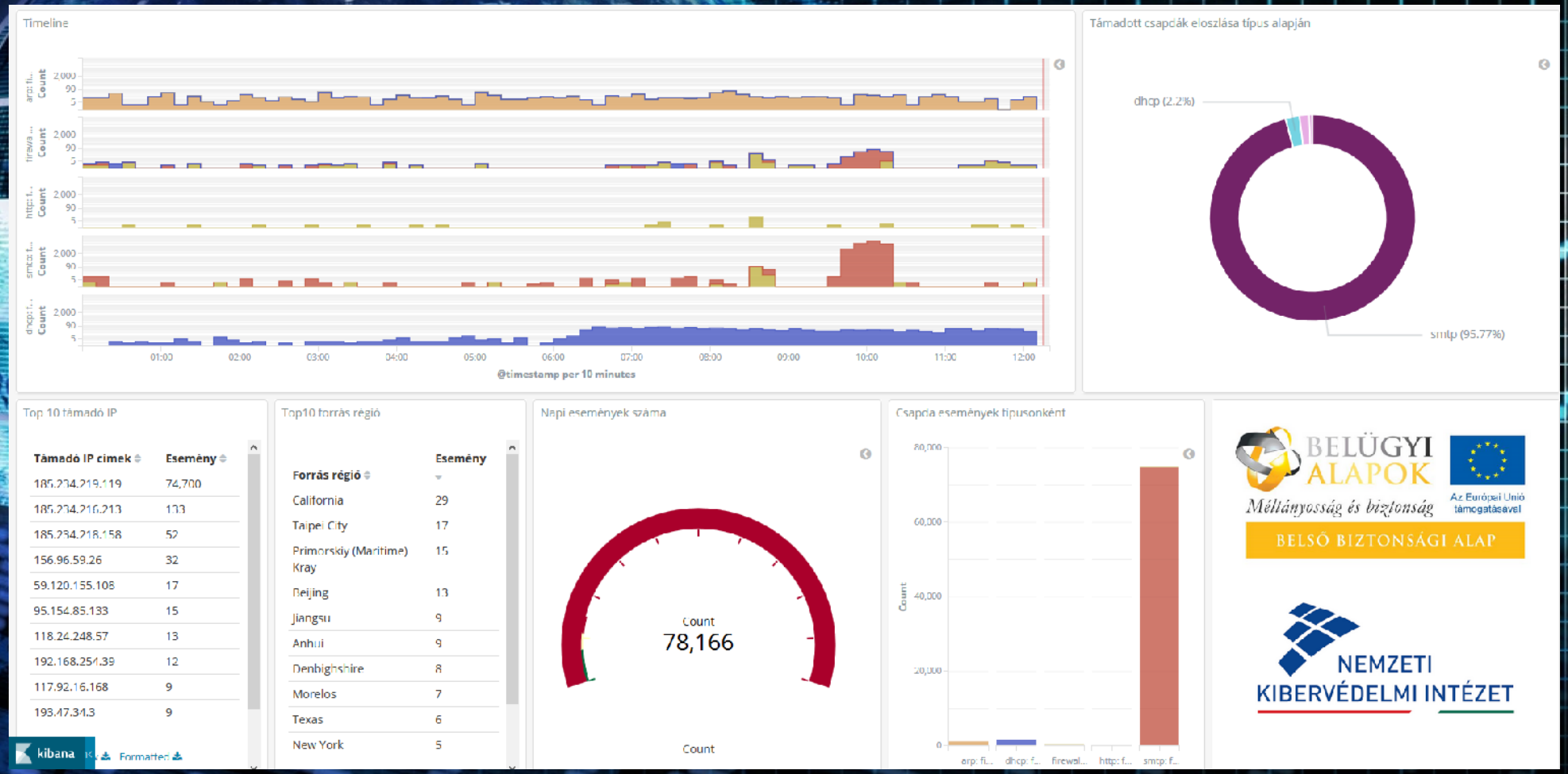
DNS

HTTP

POP3, IMAP, SMTP

honeypot - vizualizáció

Kibana



Honeypot – JELLEMZŐ STATISZTIKA

2020. február hónapban:

összesen **3.591.819** db, óránként **5.159** db csapda esemény

13.333 db egyedi forrás IP cím

28 db SMTP bejelentkezési azonosító, **9** db SMTP jelszó próbálkozás

6.550 db önálló HTTP munkamenet

2020. március hónapban:

Összesen **5.922.948** db, óránként **7.960** db csapda esemény

42.541 db egyedi forrás IP cím

5.929 db SSH bejelentkezési azonosító, **14.881** db jelszó próbálkozás

5.961 db önálló HTTP munkamenet

2020. április hónapban:

Összesen **10.838.541** db, óránként **15.053** db csapda esemény

66.204 db egyedi forrás IP cím

4.773 db SSH bejelentkezési azonosító, **19.869** db jelszó próbálkozás

9.525 db önálló HTTP munkamenet

Honeypot – KIEMELT ESEMÉNYEK

2019. május 17 – 2019. május 19.:

SSH csapda események

gyenge jelszóval védett IoT eszközökből álló botnet

SSH TCP forwarding

2019. május 08. és 2019. szeptember 01-03.:

SMTP csapda események

nagy volumenű bejelentkezési kísérlet

folyamatosan:

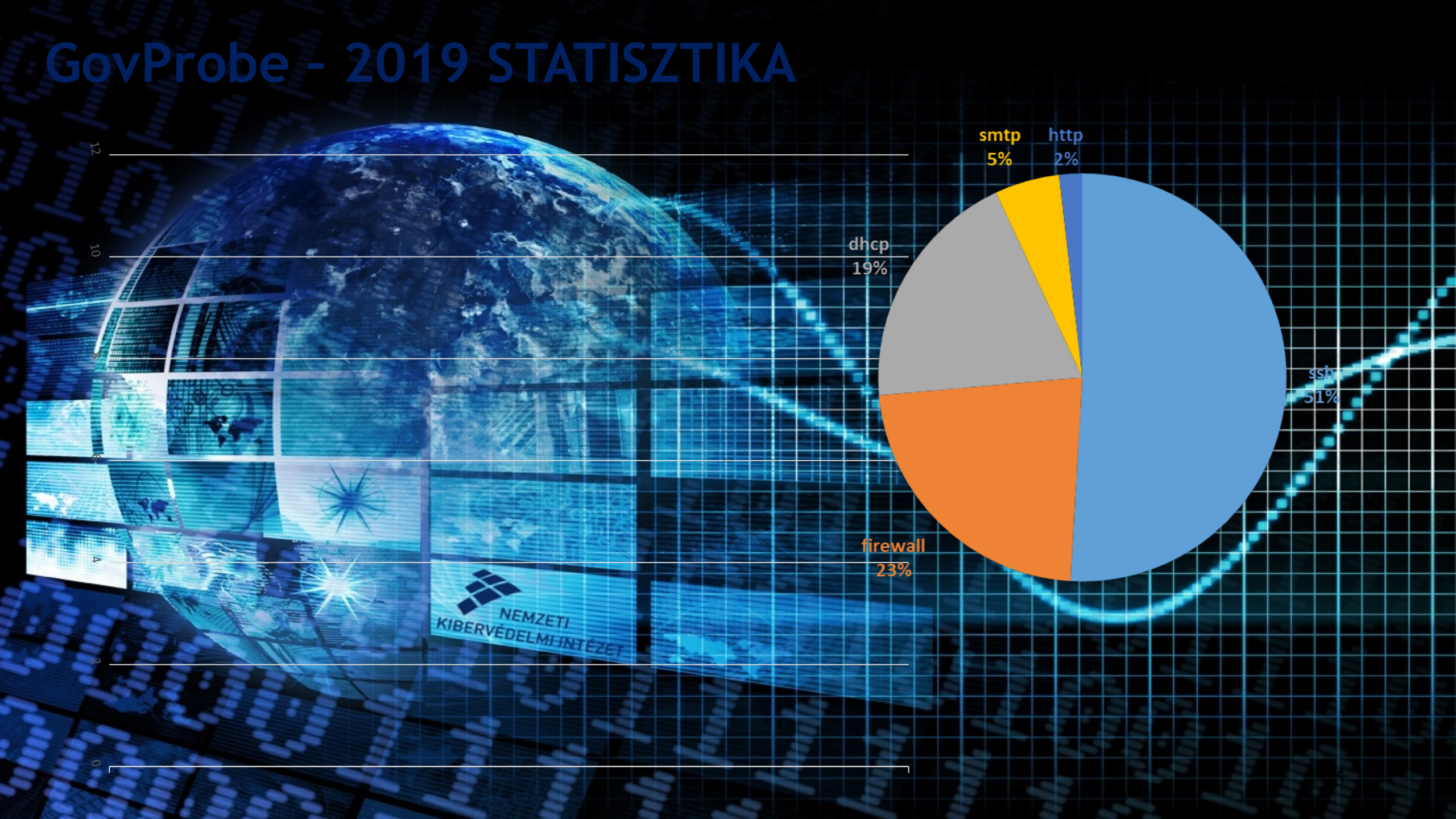
HTTP csapda események

PHP távoli kódfuttatást (RCE) lehetővé tevő sérülékenysége

nginx webszerver RCE sérülékenysége

CCTV eszközök RCE sérülékenysége

GovProbe - 2019 STATISZTIKA



Honeypot - A jövő

- Honeypot mindenkinek - virtualizáció
- Új csapdák
  - Windows
  - Magas interakciójú csapdák
  - Még több szolgáltatás modellezése
  - PLC
  - Sérülékenyeny eszközök
- Honeypot portal
- Projekt szélesítése


Köszönöm a figyelmet!
edt@nki.gov.hu
NEMZETI
KIBERVÉDELMI INTÉZET