Hungaro DigiTel
Mit kezdesz a LOGokkal

Zautasvili Péter
műszaki igazgató
Hungaro DigiTel Kft.

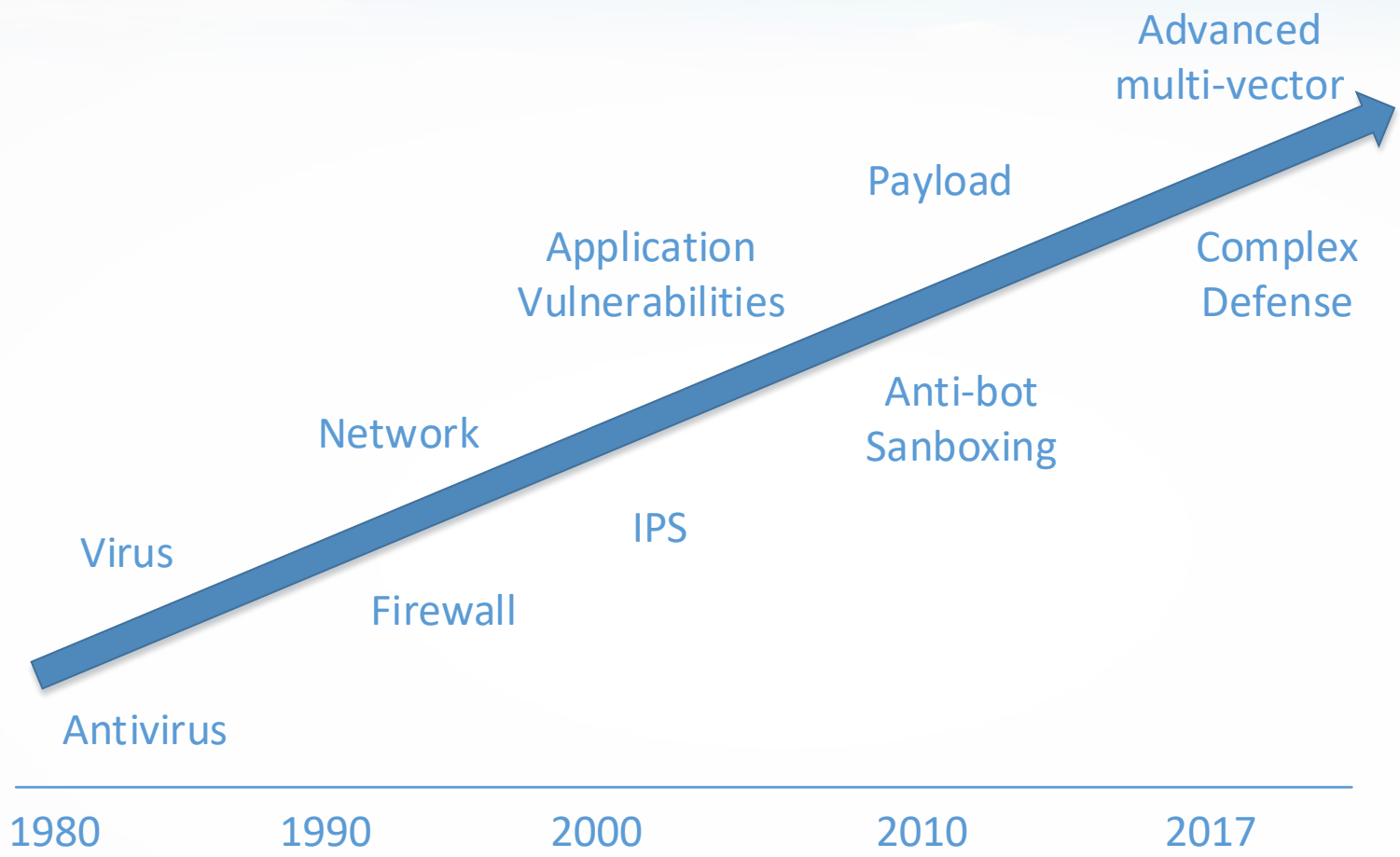
November 2018

Hungaro DigiTel - Bemutatkozás

- Hungaro DigiTel (HDT) Kft. egy magyar-portugál tulajdonú vállalat
- Európa vezető VSAT szolgáltatója és már 25 éve a piacon van
- Az utóbbi években jelentős IT és IT Biztonsági projekteket valósított meg

- Wifi központi menedzsment platform
- VVB2017 IT biztonsági megoldás szállítója
- DDoS védelmi szolgáltatások biztosítása
- Határvédelmi megoldások
- Log elemzés
- SOC

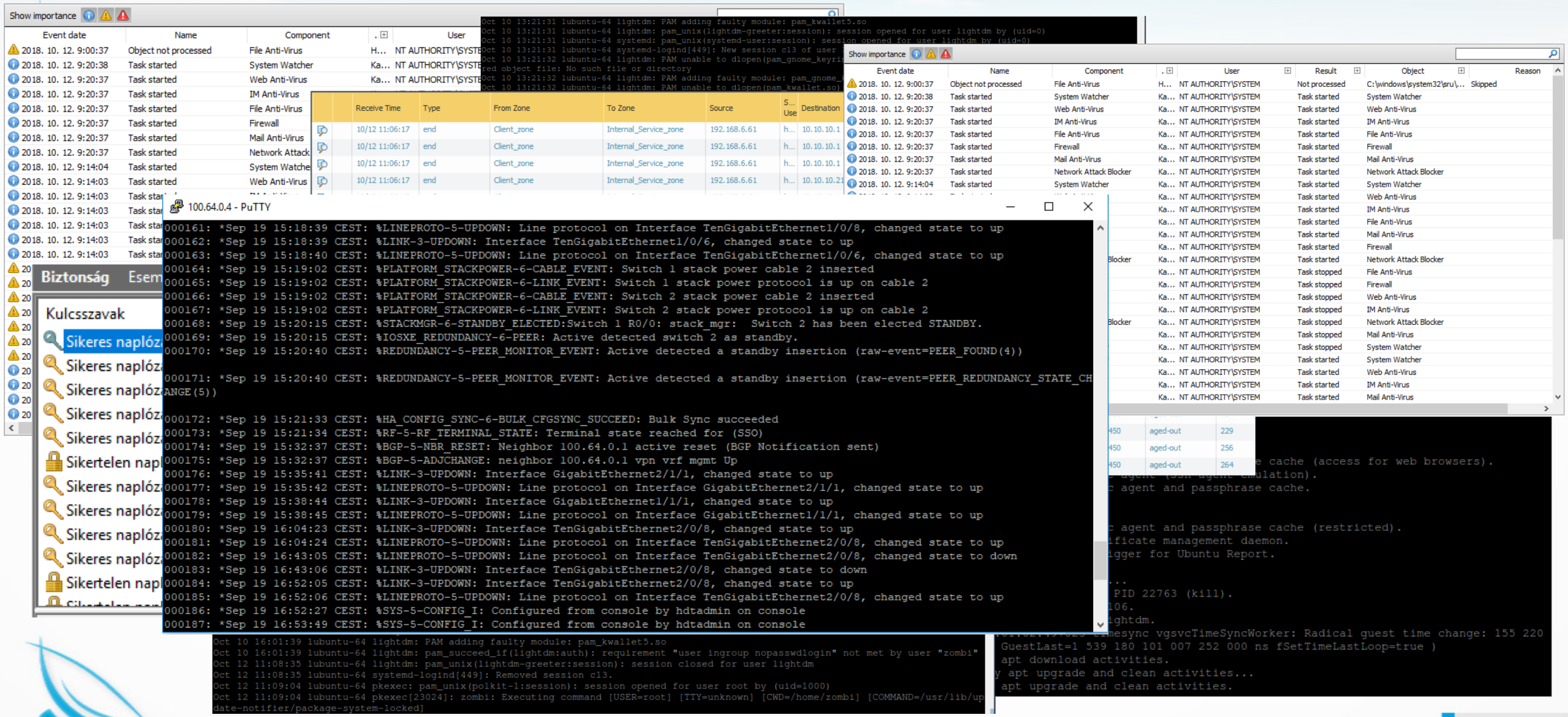
Kibertámadások fejlődése



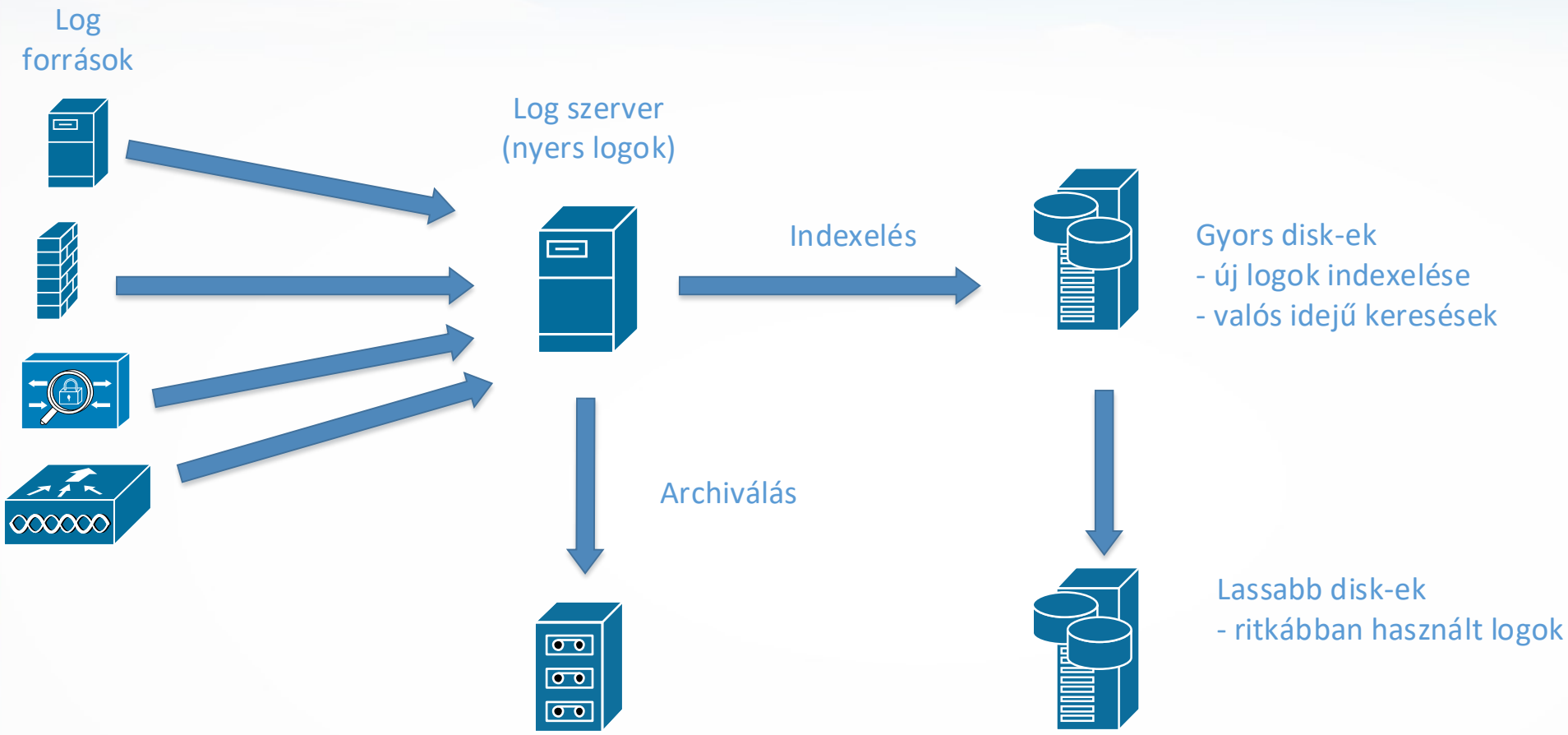
Hogyan védekezzünk?

- Tűzfalak,
- Behatolás védelmi eszközök (IPS)
- Proxy-k, WAF-ok, Email szűrők
- Végponti védelemi rendszerek
- DDoS védelemi megoldások
- Sérülékenység vizsgálók
- Titkosító eszközök
- Email szűrők
- IDM, MDM, DLP

Mit kezdünk a logokkal?



Tárolás


Log
források
Log szerver
(nyers logok)
Indexelés
Gyors disk-ek
- új logok indexelése
- valós idejű keresések
Archiválás
Lassabb disk-ek
- ritkábban használt logok

Keresés

Ki? Mit? Mikor?

SIEM

Dashboard, Korreláció, Threat feed, Riasztás, Riportok

+

SOC

Folyamatos monitorozás, Biztonsági szakértelem, Incidens kezelés,

Thank you for your attention

Contacts:

Hungaro DigiTel Plc.

2310 Szigetszentmiklós-Lakihegy

Komp u. 2.

Hungary

info@hdt.hu

https://www.hdt.hu/en/