

Hungaro DigiTel

Mit kezdés a LOGokkal

Zautasvili Péter
műszaki igazgató
Hungaro DigiTel Kft.

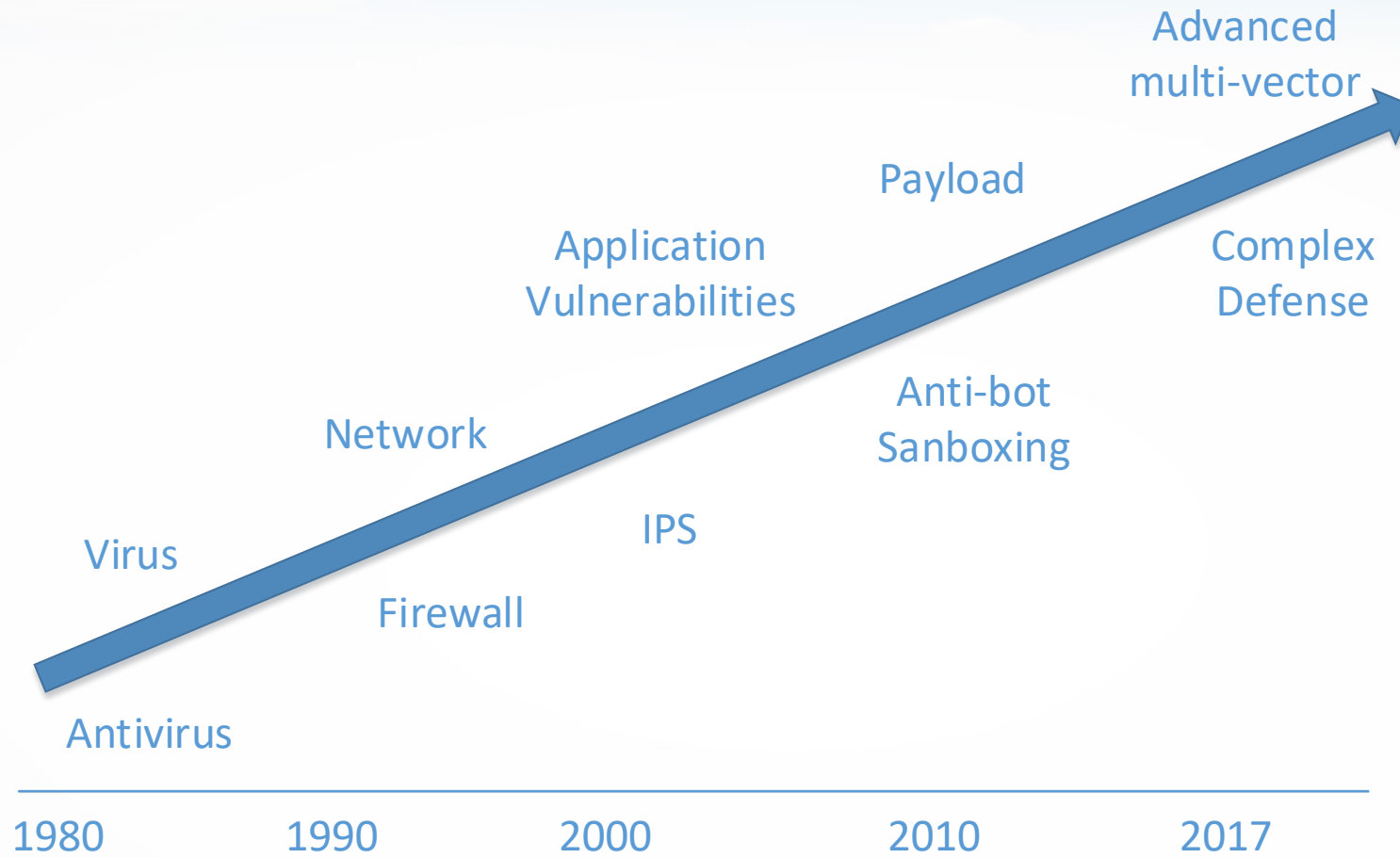
Hungaro DigiTel - Bemutató

- 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 védekezünk?

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



Mit kezdünk a logokkal?

The image shows a complex system log interface. At the top, there's a header with 'Show importance' and several warning icons. Below this, a table lists log events with columns for 'Event date', 'Name', 'Component', 'User', and 'Result'. The table contains entries for various system services like 'File Anti-Virus', 'System Watcher', 'Web Anti-Virus', 'IM Anti-Virus', 'File Anti-Virus', 'Firewall', 'Mail Anti-Virus', and 'Network Attack Blocker'. A secondary table below the main one has columns for 'Receive Time', 'Type', 'From Zone', 'To Zone', 'Source', 'S... Use', and 'Destination', showing network-related events.

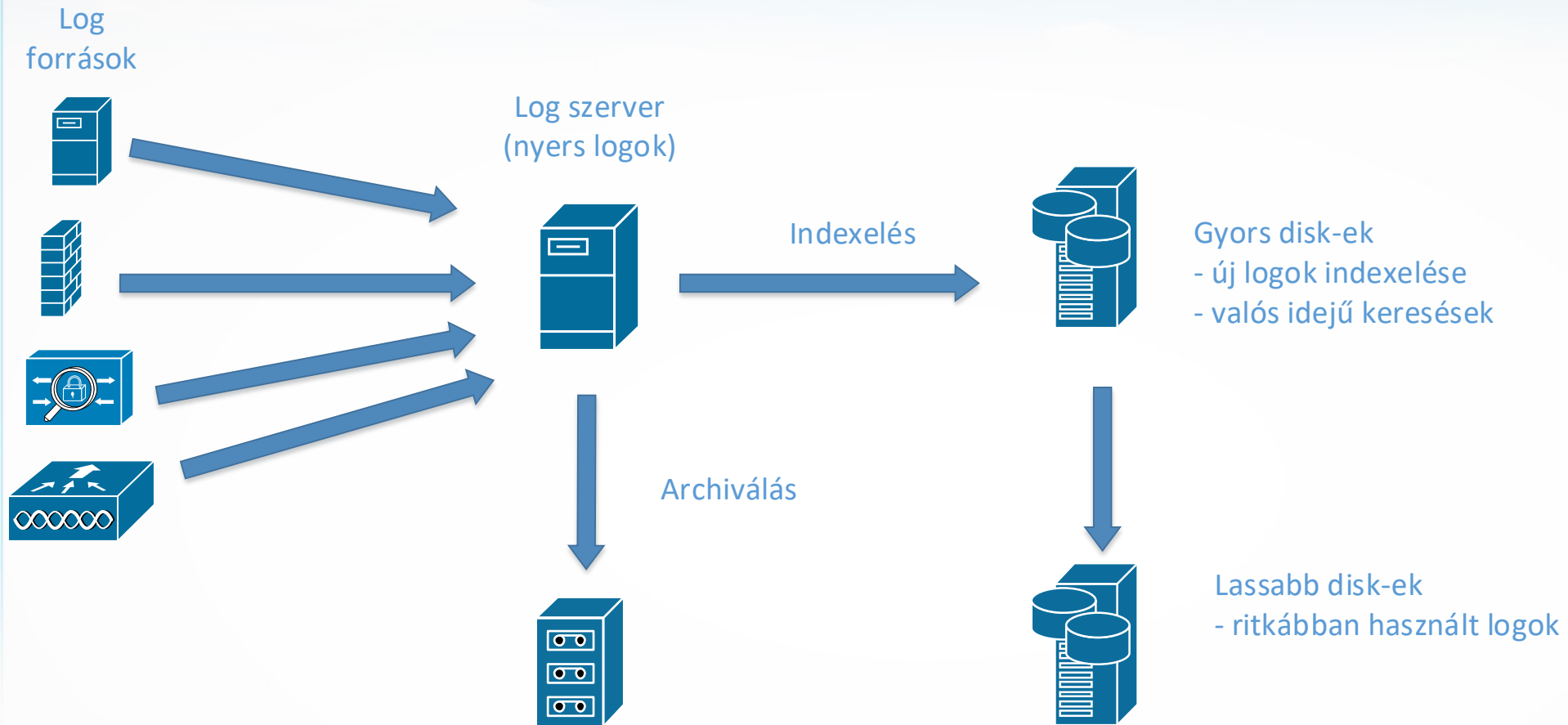
On the left side, there are several overlays: a 'Biztonság Esem...' (Security Events) panel with a list of events and their severity (e.g., 'Sikeres naplózás' - Successful logging), and a 'Kulcsszavak' (Keywords) panel with a search bar and a list of terms like 'Sikeres naplózás', 'Sikertelen naplózás', etc.

The main terminal window displays a large block of log output in a monospaced font, showing detailed system messages such as 'LINEPROTO-5-UPDOWN: Interface TenGigabitEthernet1/0/8, changed state to up' and 'LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/6, changed state to up'. There are also some smaller terminal windows visible, including one titled '100.64.0.4 - PuTTY'.

At the bottom right, there's a small table with columns for 'aged-out' and a numerical value, showing values like 229, 256, and 264. Below this, there's a snippet of code or configuration related to 'timesync vgsvcTimeSyncWorker'.



Tárolás



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/>

