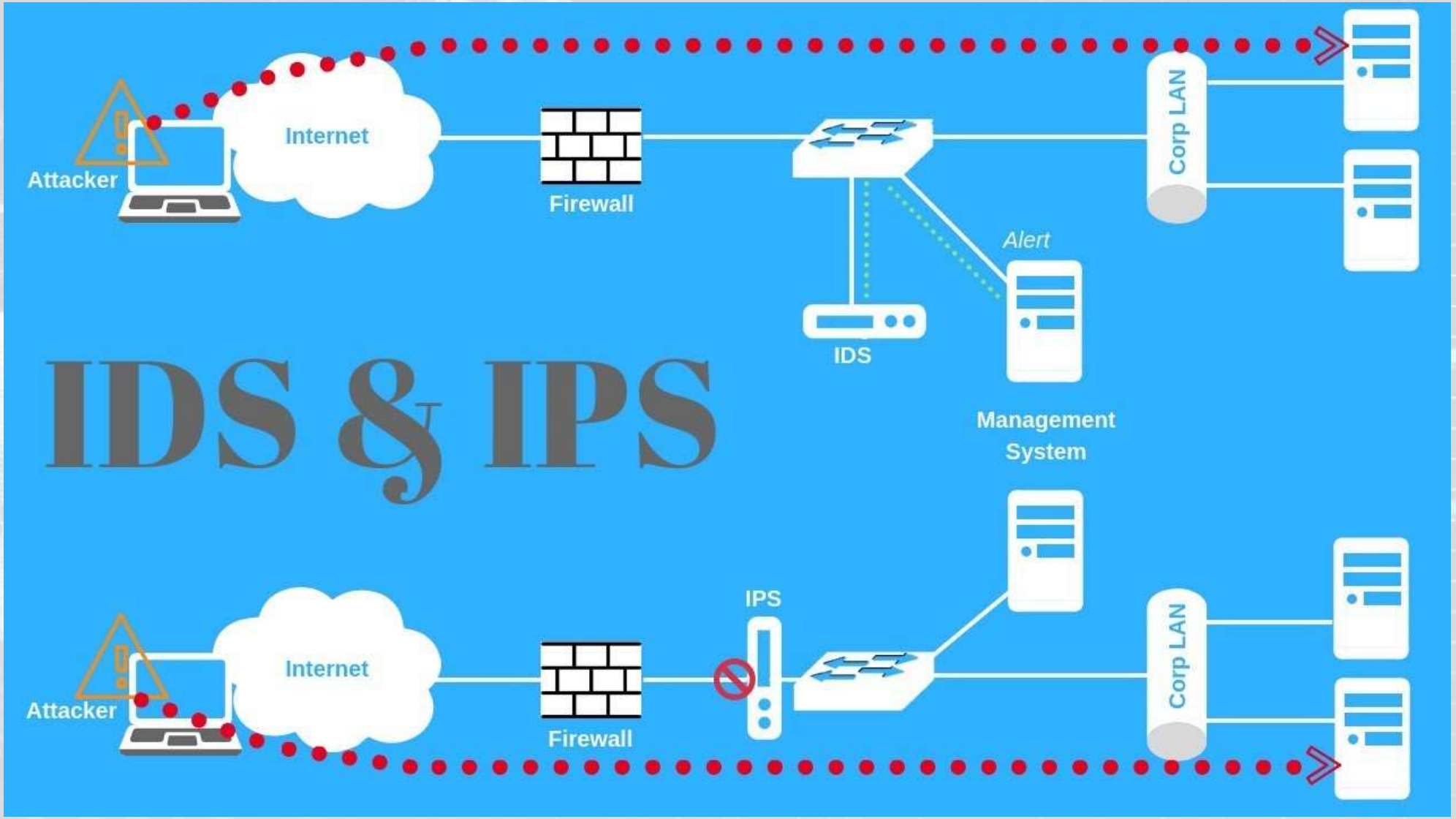
IDS/IPS és NKI-EWS

Marsi Tamás

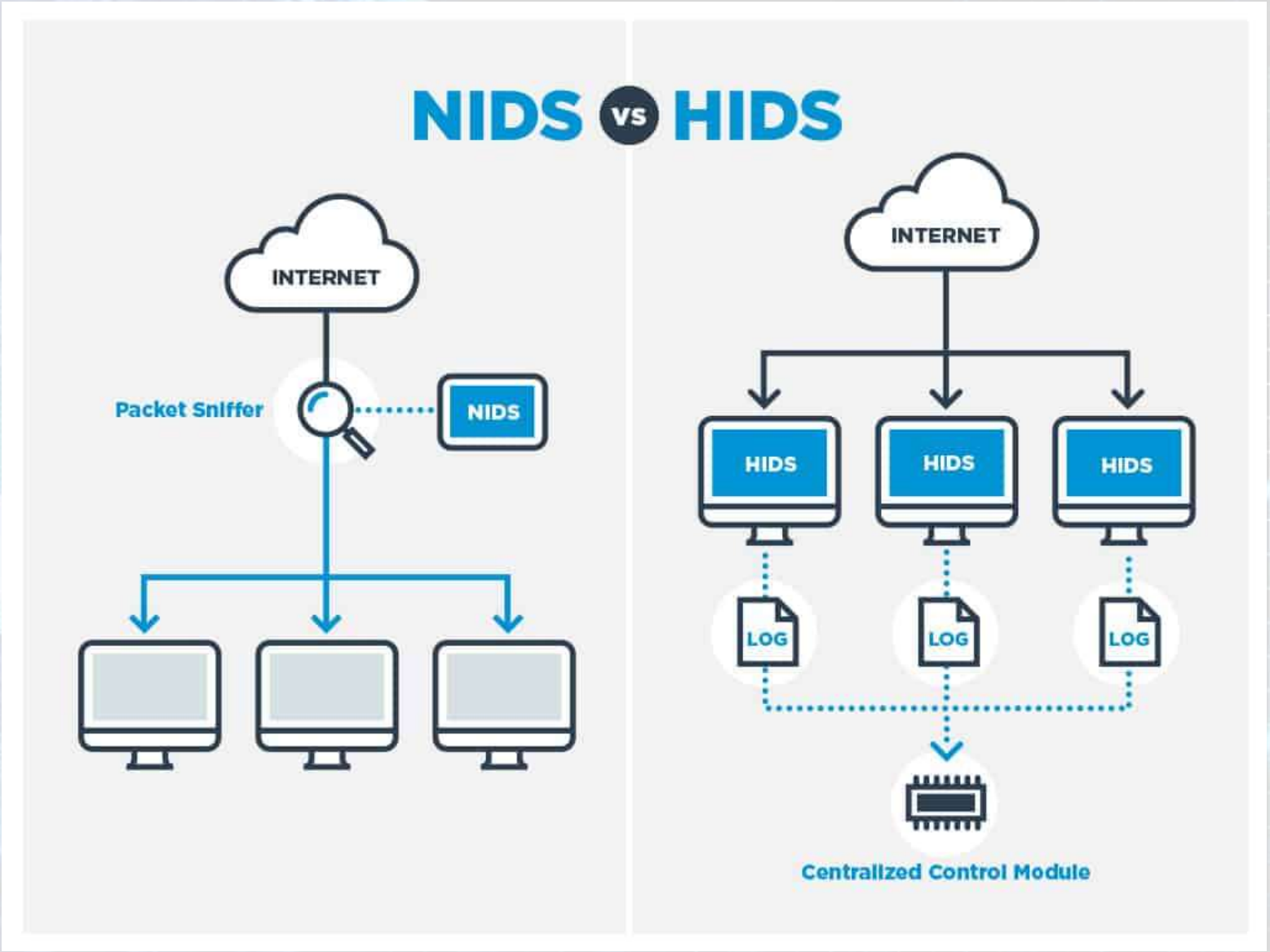
TARTALOM

- IPS-ek
- IDS-ek
- EWS
- Kormányrendelet

IPS VS. IDS


IDS & IPS
Attacker
Internet
Firewall
IDS
Alert
Management System
Corp LAN
Attacker
Internet
Firewall
IPS
Corp LAN

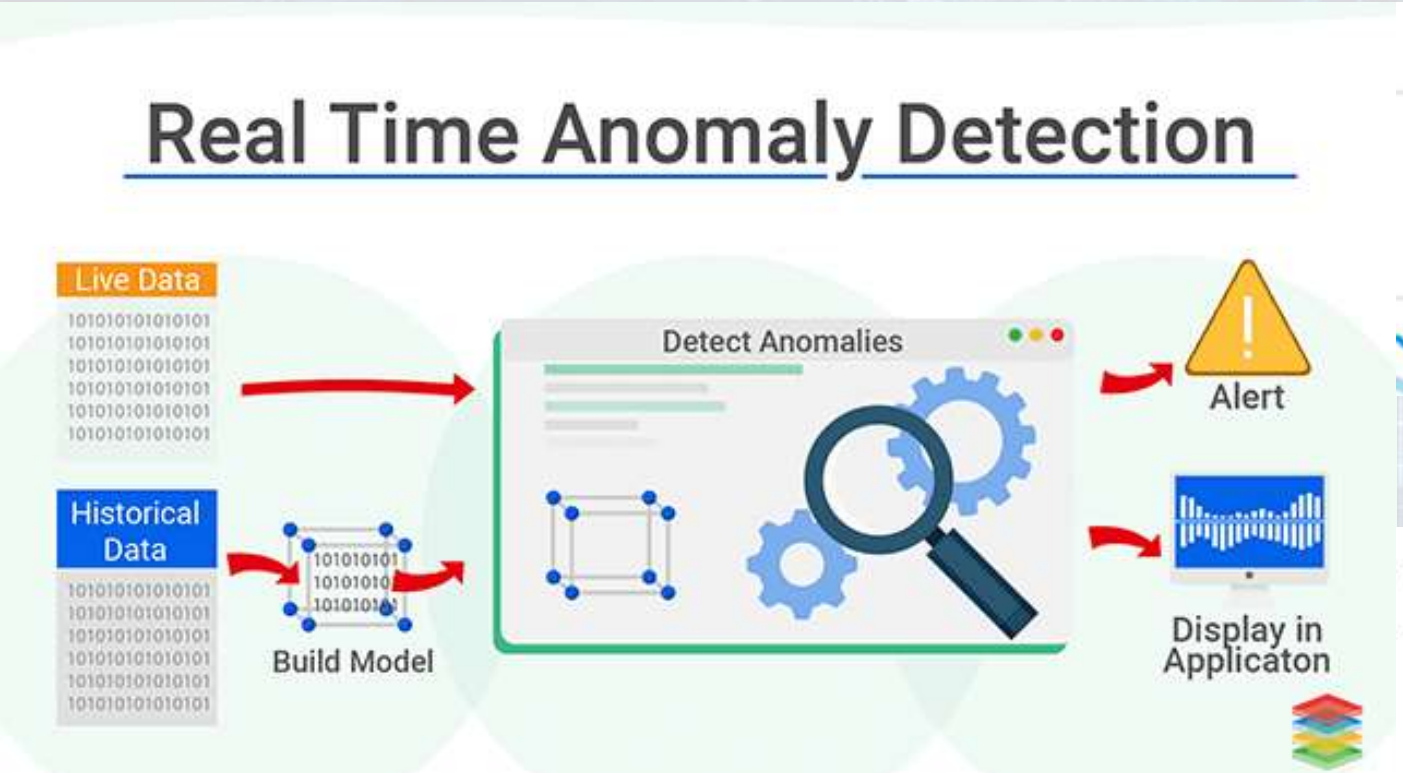
NIDS VS. HIDS

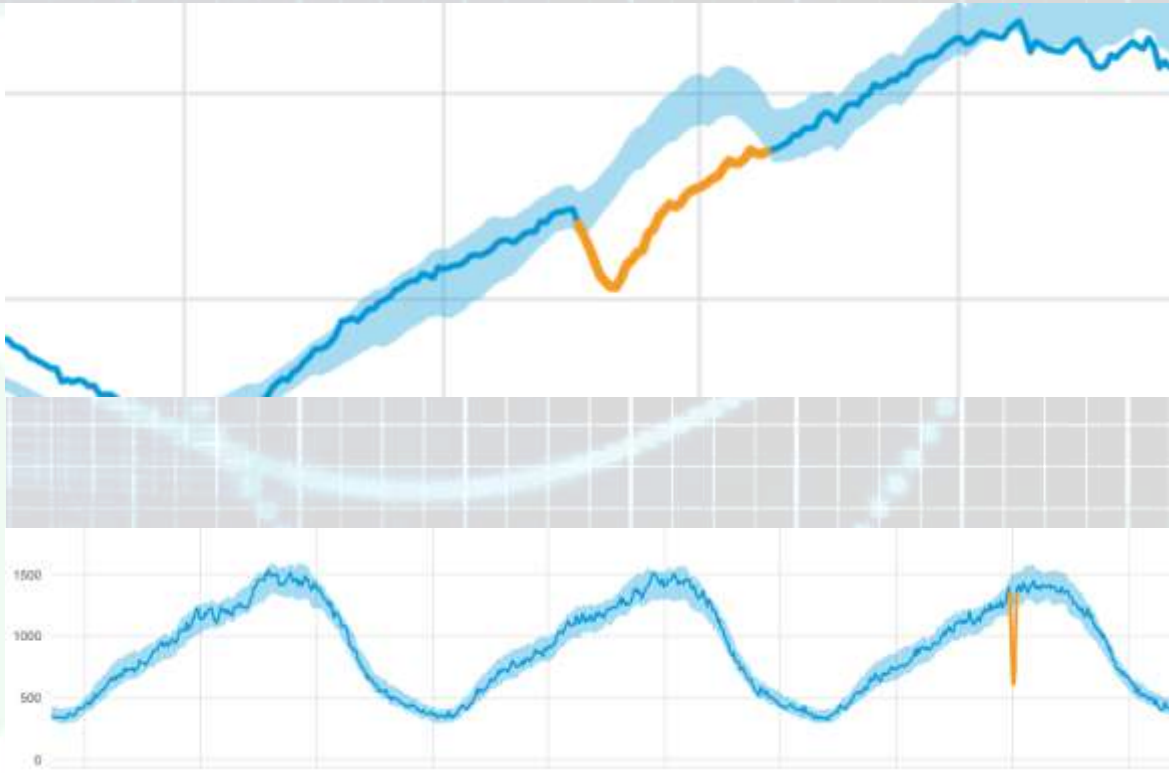

NIDS VS HIDS
INTERNET
Packet Sniffer
NIDS
INTERNET
HIDS
HIDS
HIDS
LOG
LOG
LOG
Centralized Control Module

SZIGNATÚRADETEKCIÓ

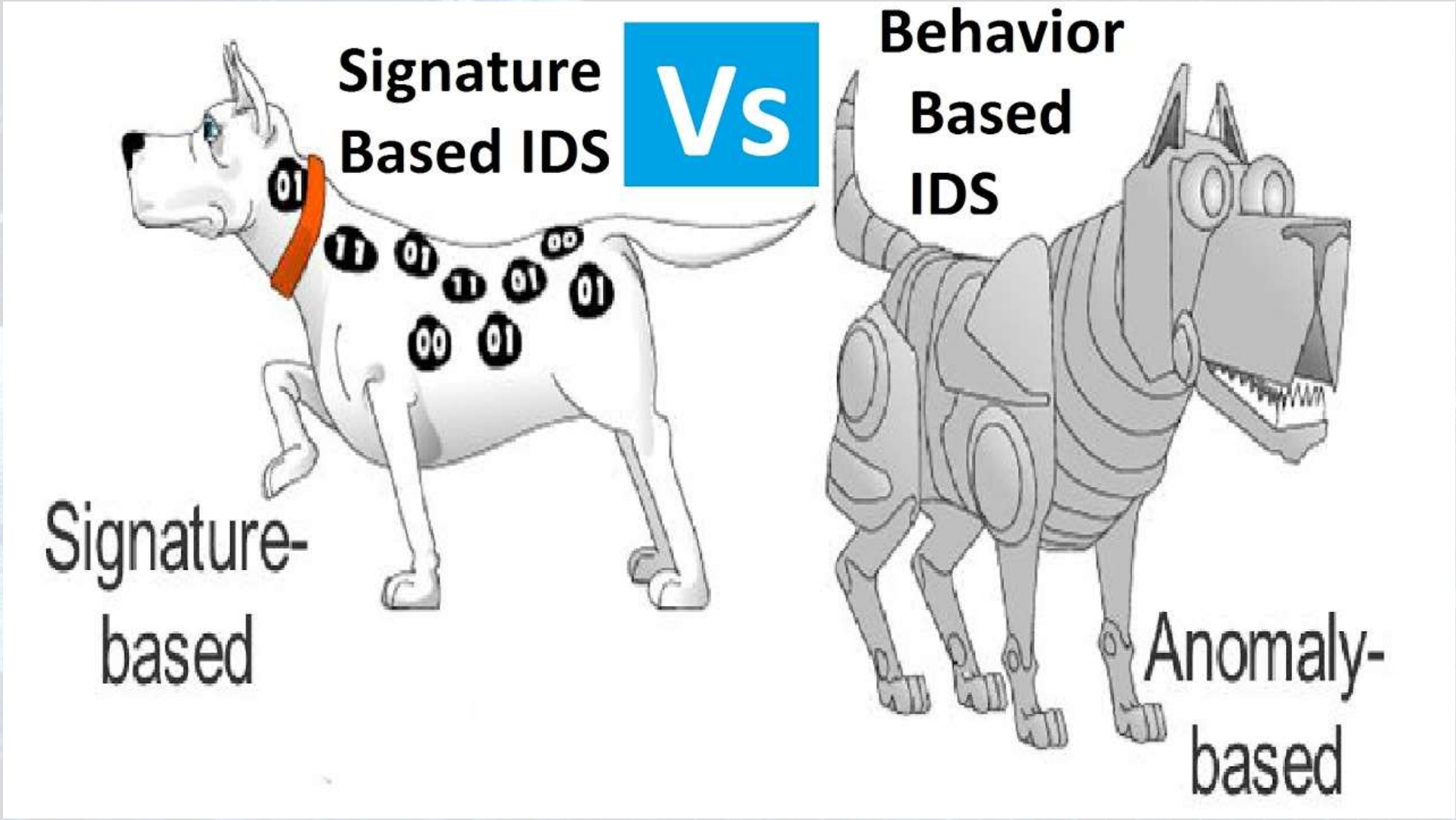

```
.00402FF0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403000:  6B 65 72 6E.65 6C 33 32.2E 64 6C 6C.00 57 69 6E  kernel32.dll Win
.00403010:  45 78 65 63.00 52 65 67.69 73 74 65.72 53 65 72  Exec RegisterSer
.00403020:  76 69 63 65.50 72 6F 63.65 73 73 00.75 72 6C 6D  viceProcess urlm
.00403030:  6F 6E 2E 64.6C 6C 00 2D.2D 2D 2D 2D.2D 2D 2D 2D  on.dll ---------
.00403040:  2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 00.00 52 4C 44  ----------  RLD
.00403050:  6F 77 6E 6C.6F 61 64 54.6F 46 69 6C.65 41 00 2D  ownloadToFileA -
.00403060:  2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D  ----------------
.00403070:  00 68 74 74.70 3A 2F 2F.6E 75 72 73.69 6E 67 6B   http://nursingk
.00403080:  6F 72 65 61.2E 63 6F 2E.6B 72 2F 69.6D 61 67 65  orea.co.kr/image
.00403090:  73 2F 69 6E.66 32 2E 70.68 70 3F 76.3D 73 00 78  s/inf2.php?v=s x
.004030A0:  78 78 78 78.78 78 78 78.78 78 78 00.68 74 74 70  xxxxxxxxxx http
.004030B0:  3A 2F 2F 6E.75 72 73 69.6E 67 6B 6F.72 65 61 2E  ://nursingkorea.
.004030C0:  63 6F 2E 6B.72 2F 69 6D.61 67 65 73.2F 6D 65 64  co.kr/images/med
.004030D0:  73 2E 67 69.66 00 63 3A.5C 34 35 39.5C 2E 65 78  s.gif c:\459\.ex
.004030E0:  65 00 63 3A.5C 62 6F 6F.74 2E 62 61.6B 00 00 00  e c:\boot.bak
.004030F0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403100:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403110:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
```

ANOMÁLIADETEKCIÓ

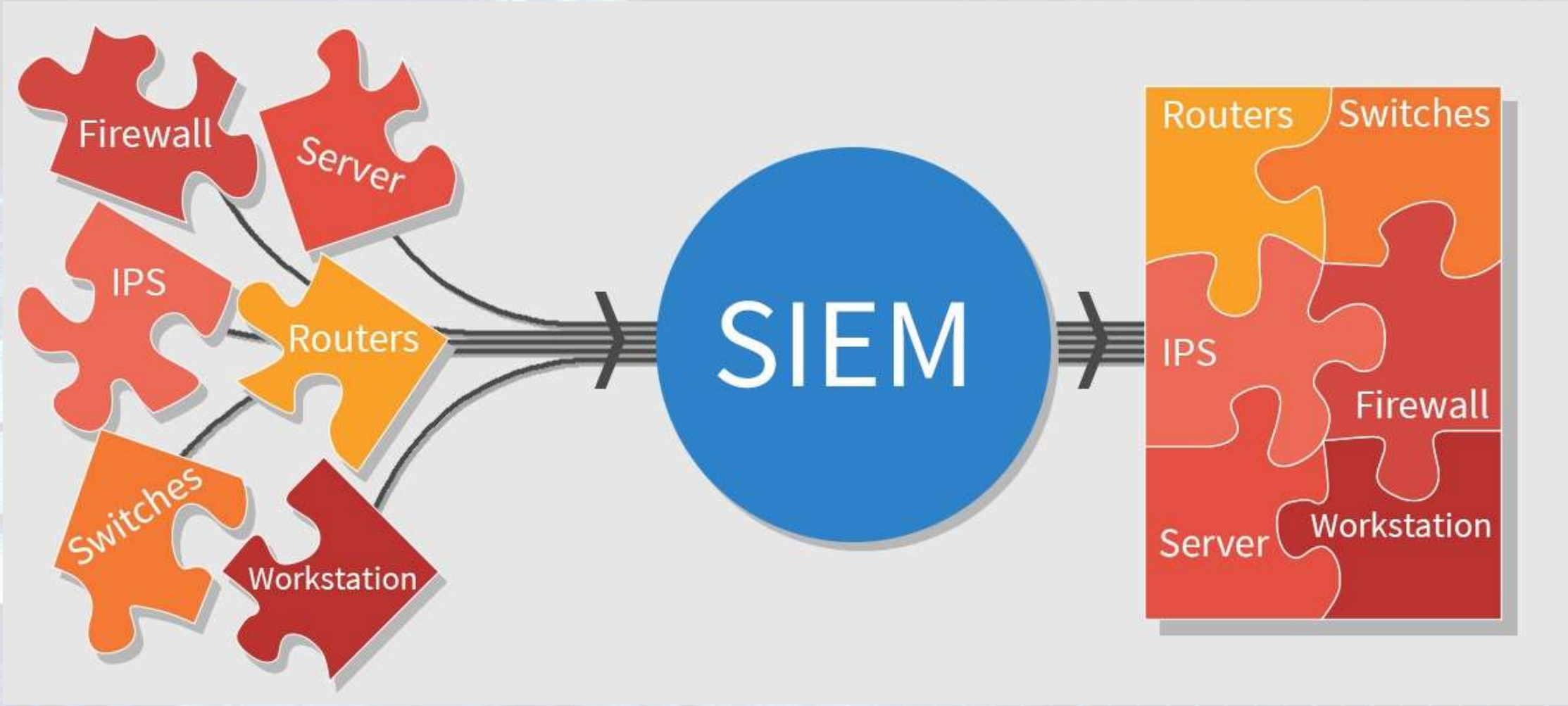




ANOMÁLIA VS SZIGNATÚRA



SIEM

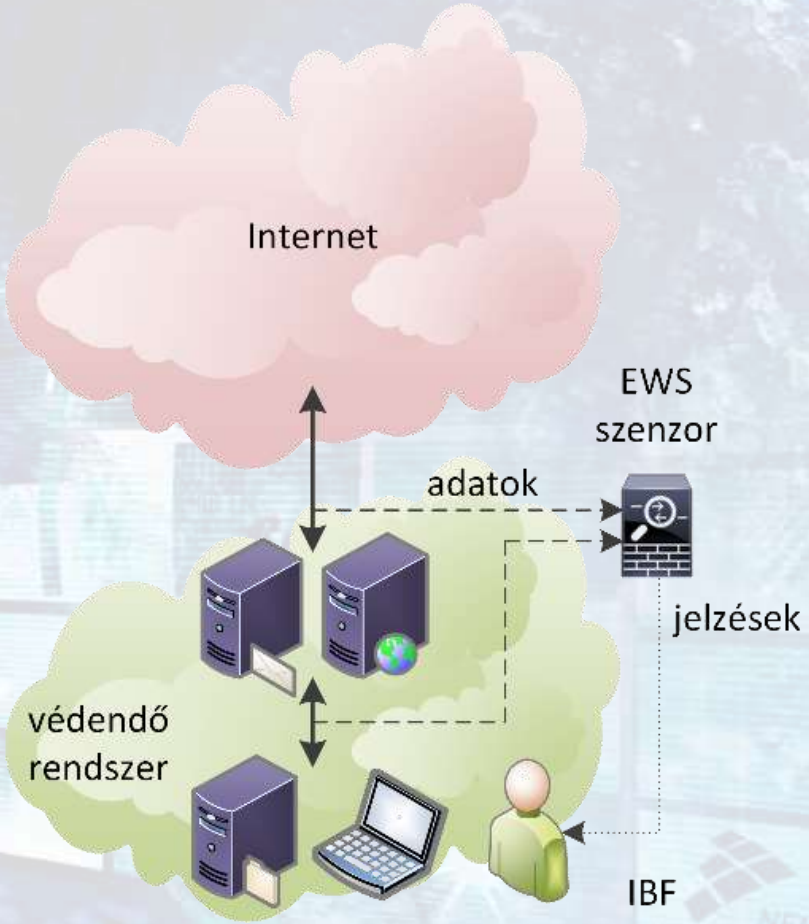

Firewall
Server
IPS
Routers
Switches
Workstation
SIEM
Routers
Switches
IPS
Firewall
Server
Workstation

SOC

EWS

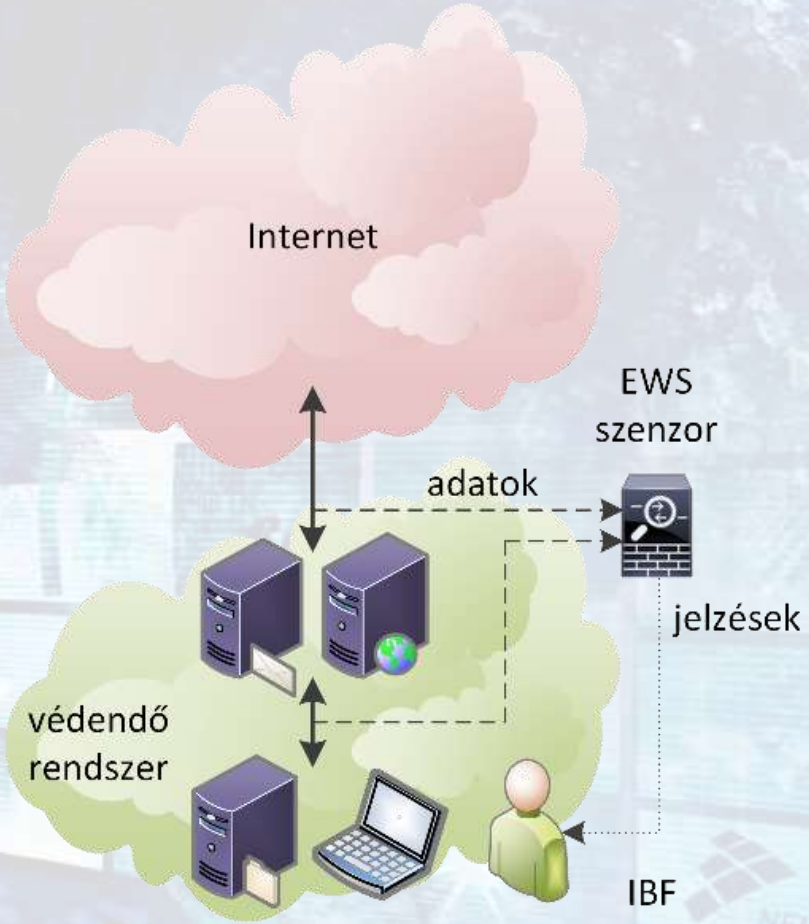
- EWS: Early Warning System
  - Nemzetközi minták alapján
  - Központosított hálózatbiztonsági felügyeleti szolgáltatás
- Definíció
  - Egyirányúan összekapcsolt
  - Információs rendszerek hálózati forgalma
    - Elemzés
    - Kockázatok azonosítása
    - Támadás, visszaélés, kísérlet azonosítása

EWS



- EWS – adatgyűjtés
  - Szolgáltatás nyújtása
  - NKI és védett intézmény részére
- Csatlakozás műszaki követelmények
  - Hálózati forgalom átadása (tap/mirror)
  - Titkosítás feloldása
  - Kritikus hálózati csomópontok kialakítása
  - Naplókezelési minimumkövetelmények

EWS



- Több, mint IDS
  - Riasztások
  - Netflow
  - Nyers hálózati forgalom
  - Elemzési lehetőség
- EWS szenzor
  - IDS: Suricata
  - Forgalomgyűjtés és elemzés: Moloch
- Központi rendszer
  - Elastic – kibana
  - Támogató portál

EWS ELŐNYÖK

- Korszerű technológia
- Csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhek
- Gyorsul a támadásokkal kapcsolatos reakció képesség
- Saját ticketing funkció
  - Nyomonkövetés
  - Incidens bejelentés az NKI-CSIRT-nek
- GDPR kompatibilis
- Folyamatosan aktuális szabálykészlet

EWS KORMÁNYRENDELET

- 214/2020. (V. 18.) Korm. Rendelet
- Főbb tudnivalók:
  - IBTV jogosultak és egyéb szereplők vehetik igénybe
  - Kötelező a KAK-ra kötelezett rendszerek esetén
  - Üzemeltetését az NKI biztosítja
  - Csatlakozási költség az intézményt terheli
- NISZ-KAK csatlakozás:
  - Egyszerű, mert eszközök rendelkezésre állnak
  - SSL terminálás a KAK tűzfalon
  - Tanúsítvány átadása a NISZ-nek

Köszönöm a figyelmet!

nki.gov.hu/ews
cert@nki.gov.hu