Nemzeti Média- és Hírközlési Hatóság

# *A CTI szerepe az NMHH IT biztonsági üzemeltetésében*

EIVOK 47

## Hatósági IT

- Minden munkavégzés valamilyen IT támogatással történik
  - Mindent átszövő jellege miatt különleges helyet foglalunk el

- Ez a lehetőségek mellett kockázatokkal is jár
  - Fontos, hogy a felhasználók ne kényelmetlenségként éljék meg a munkánk – akkor jó, ha nem is tudják, hogy vagyunk
  - Az IT-nek képesnek kell lennie proaktív módon felismerni a kockázatokat és reagálni rájuk

## CTI munkatársként

- Hogy néz ki az üzemeltetés szintjéről?
- Autonómia, alacsony kitettség
- Hogyan lesz gyors, hatékony és kényelmes?

- Növekvő fenyegetettség – szinte bárki lehet támadás célpontja

Az üzemeltető szempontjai, az Informatikai Biztonsági Stratégián túl

- A saját munkánk könnyebbé tétele
- A reakcióidő lerövidítése
- A várható támadások észlelése, lehetőség szerint megelőzése
- Nagyobb felhasználói elégedettség elérése

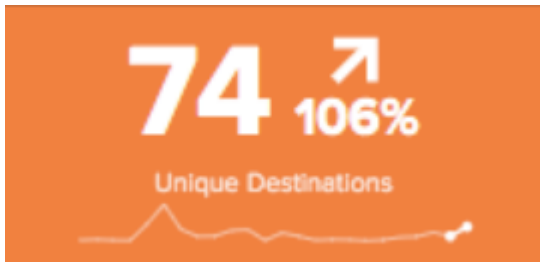
# Log, én vagyok az apád

- Logolás – vagy annak hiánya
- Nagy mennyiségű adat a monitoring rendszerekből
- A feldolgozást segítő eszközünk a Splunk

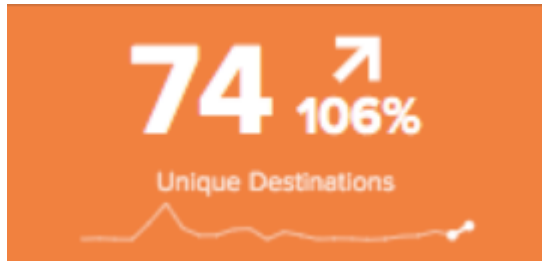
# *A CTI szerepe az NMHH IT biztonsági üzemeltetésében*
Három gyakorlati eset

## SPAM

- Mennyiségi monitorozás
- Jelezheti, hogy kampány áldozatai lehetünk
- Gyanús levelek elemzése szeparált környezetben
- Hash ellenőrzések
- Steghide – sztegonográfia
- Threat db-k
- Browserling



## SPAM – a jövő (és az üzemeltető álmai)




- Az Informatikai és Informatikai Biztonsági Stratégia meghatározott célja az AI fokozatos bevonása
- AI alapú támadások ellen AI védekezés
- Felhasználó/Viselkedés alapú AI elemzés a tartalomelemzés mellett

- AI alapú DLP

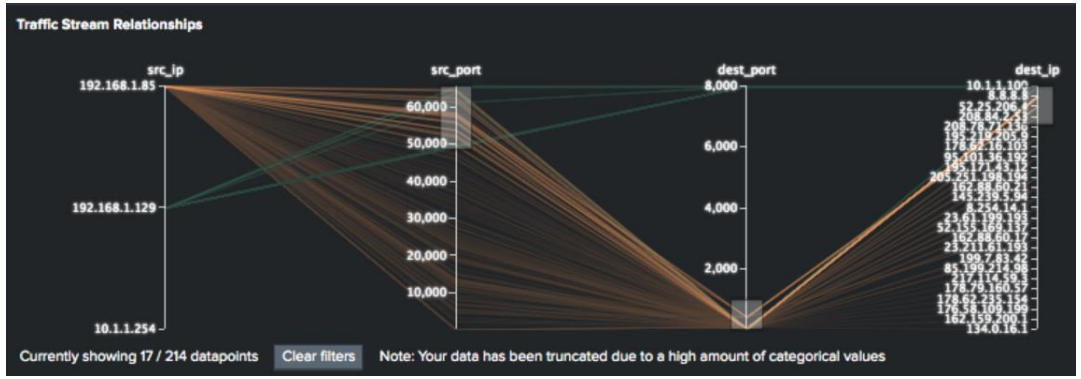
    - Mit akarunk az AI-jal

# Három gyakorlati eset

## Mérőállomások forgalmának mérése

- Mennyiségi mérés, új forgalom megjelenése
- Teljesítmény anomáliák
- Sessionök száma

- Gyanús írás/olvasás arány
- Szokatlan kapcsolatok
- Scannelés



# Három gyakorlati eset

## Mérőállomások forgalmának mérése

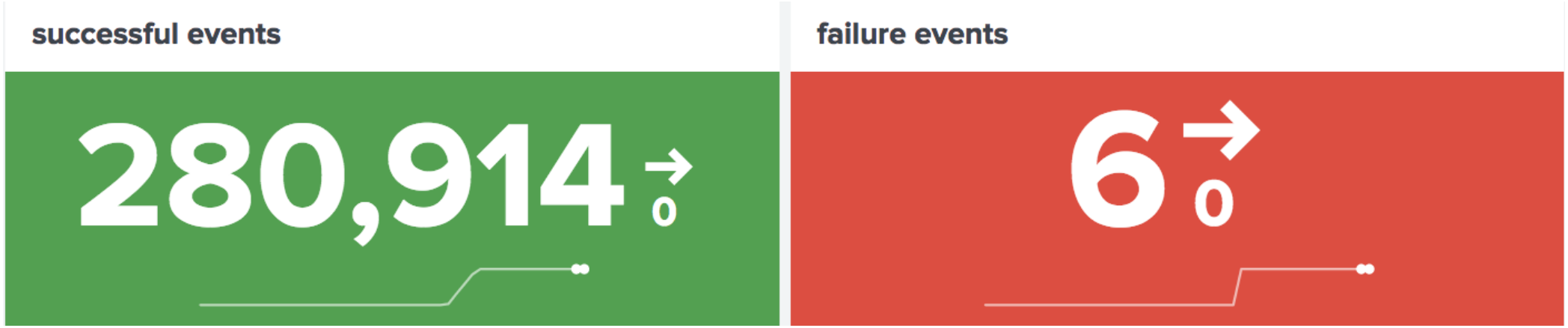
- Mit szeretnénk a jövőtől?

- Az előző dián felsorolt nyers adatból AI segítségével döntést hozni, és ellenlépést tenni
- Megelőzés, észlelés és választevékenység AI segítséggel

# Három gyakorlati példa

## Mit mondanak a user loginok

- Hibás loginok mennyisége
- Milyen felhasználók érintettek
- Honnan próbálkoznak



# *A CTI szerepe az NMHH IT biztonsági üzemeltetésében*
## Három gyakorlati példa

Mit szeretne az üzemeltető?

- AI alapú észlelés és elemzés
- AI által segített ellentevékenység (Felhasználó gyanús tevékenységének felderítése és megakadályozása, hasonló mintákat mutató felhasználók észlelése, összefüggések átfogó keresése)

## NMHH mint lakossági CTI szolgáltató

- KiberPajzs projekt
- Digipedia.hu
  - Gyerekvédelem, online pénzügyek, netes veszélyek, adatvédelem

Nemzeti Média- és Hírközlési Hatóság

# Köszönöm megtisztelő figyelmüket!