# Nagy mennyiségű CTI hatékony feldolgozása

**Sági Gábor**
SOC vezető
NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

**2024.05.02.**

# Mit tekintünk CTI-nak

A fenyegetés-intelligencia (CTI – Cyber Threat Intelligence magyarul inkább **fenyegetettségi információ**k és azok **feldolgozása**) az ellenfelekről és azok motivációiról, szándékairól és módszereiről szóló tudás, amelyet olyan módon gyűjtünk, elemezünk és terjesztünk, hogy minden szinten segítsenek az üzleti és a biztonsági területeknek megvédeni a vállalat kritikus eszközeit (beleépre az adatainkat) és segítünk másoknak is ezen tevékenyégben
+ sérülékenységi információk

# Stratégia szint kihívásai

- A szervezet nem mindig tudja, hogy mik a valós fenyegetések és mely kockázatokkal lehet és kell számolni - Threat Landscape
- Sok-sok fajsúlyos és hosszú dokumentum készül, sok-sok szempontból, de
  - Nem minden releváns
  - Nem feltétlen kormányzati fókuszú dokumentumok
- Hosszabb távú gondolkodás szükséges
- Kevés olyan szakember van, aki stratégiai és technikai oldalon is erős
- A vezetőknek el kell tudni mondani, hogy mit, miért és hogyan
- Forrást kell biztosítani a megvalósításra

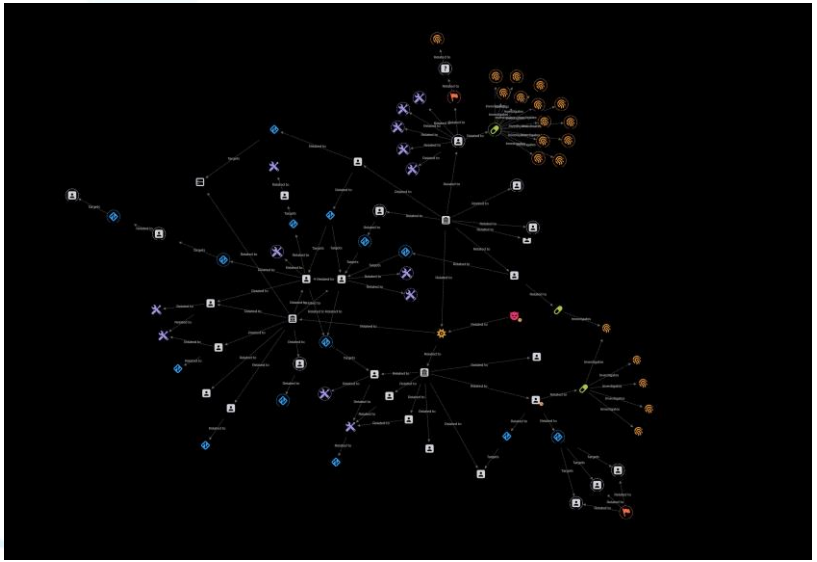
# Taktikai szint kihívásai

- Nagyon sok forrásból érkezhetnek információk
- Az információk eltérő mélységűek, sokszor egymást kiegészítve lehet hatékonyan használni
- Néha vannak ellentmondások és talán dezinformációk is
- Releváns tartalom kiválasztása néha elég nehézkes, a feldolgozás időrabló
- Manuális feldolgozás, de az eredményt „gépiesíteni” kell

# Technikai szint kihívásai

- Forrástól függően napi néhány ezertől akár 50-60 ezerig
- Csak automatikusan megoldható
- Nagyon gyorsan értéktelenné válik (akár 1-2 óra alatt is)
- Nem lehet mindent feldolgozni és talán nem is érdemes, de ki kell tudni választani, hogy mivel foglalkozzunk
- Jól ki kell találni, hogy mi mentén érdemes az automatizmusokat kialakítani
- Validáció javasolt

# És amit adni lehet…



- Mindenki mindent is szeretne, de!
- Kinek és mit adunk/adhatunk át?
- Hatékonyság az automatizmussal javítható.
- Jó, ha van egy platform!

NISZ

# KÖSZÖNÖM A FIGYELMET!