# „Konyhakész” adatelemzés

# KÜRT Zrt.
# Információbiztonság és Adatmentés

## Adatmentés

Logikailag és fizikailag sérült adathordozókról való adatmentés.

## IT biztonság, Adatvédelem

Információbiztonsági és adatvédelmi szakértői szolgáltatások, sérülékenység vizsgálatok, biztonsági tervezés, audit és tanácsadás.

## Termékfejlesztés

A felhalmozott tudás és tapasztalat újrahasznosításának legjobb módja innovatív szoftverek fejlesztése.

# Miért van szükség az adatok feldolgozására?

Az adat nagy tömegben keletkezik.

Az adatot információvá kell alakítani.

Az információ felhasználási lehetőségei:

| | | | | |
|---|---|---|---|---|
| Lehetséges veszélyek felderítése | Kártékony felhasználói tevékenység felfedése | Trendelemzés | Üzleti folyamatok elemzése | Üzleti döntések előkészítése |

# Mi az „adat” és feldolgozása?

Minden informatikai rendszer és alkalmazás adatot generál a saját működéséről.

Az adat
- rendszerek, alkalmazások által generált,
- tartalma változó és igen bőséges,
- formátuma nem szabványos.

Adatból rendkívül nehéz számunkra hasznos információt kinyerni.

Célunk az adott rendszer
- biztonsági szintjének növelése,
- működésének folyamatos hatékonyabbá tétele.

# Jelenlegi elemzési lehetőségek

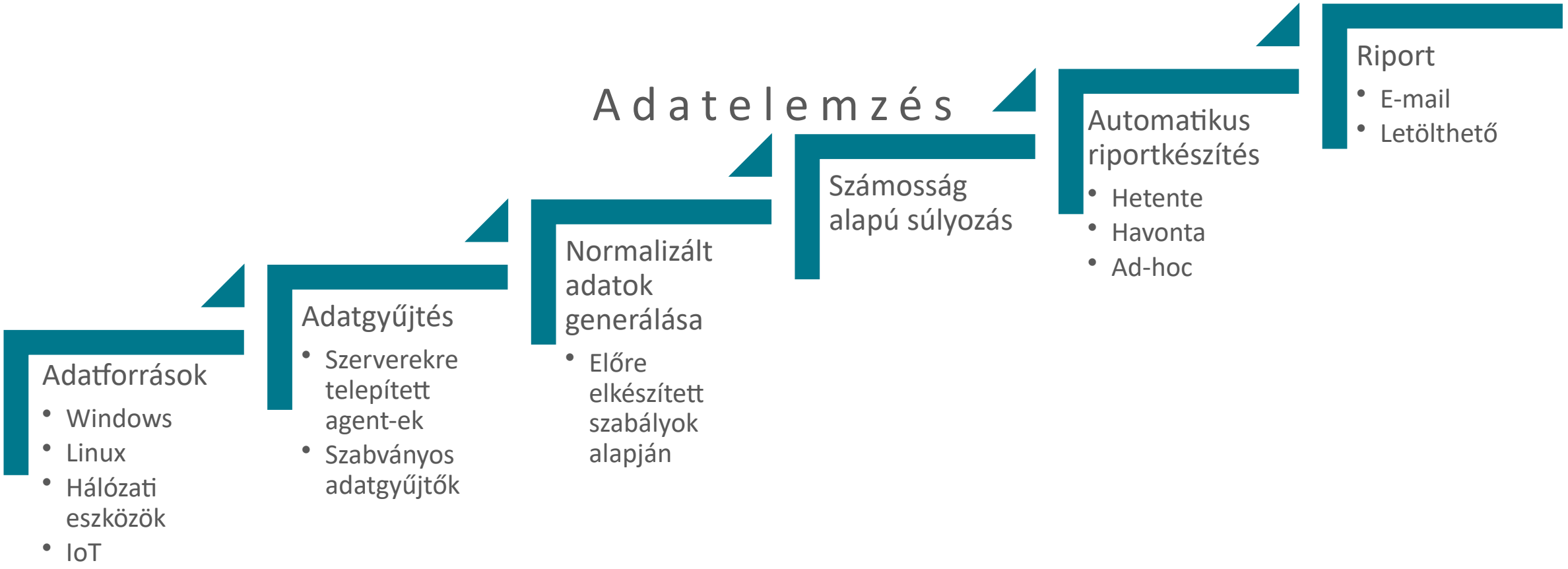
| | Manuális elemzés | Elemző alkalmazás |
|---|---|---|
| **Kihívások** | • Különleges szaktudás szükséges<br>• Rendkívül lassú<br>• Túl sok adat áll rendelkezésre<br>• A fontos információk azonosítása | • Különleges szaktudás szükséges<br>• Nagy erőforrás igényű<br>• Nehézkes testreszabhatóság<br>• Központi adattárház kell hozzá<br>• Minden eszköz különböző módon állítja elő az adatot |

# Automatizált elemző alkalmazás

- Nem igényel speciális szakértelmet.
- Riport grafikonokkal, táblázatokkal, magyarázatokkal.
- Közvetlenül informálja:
  - Információbiztonsági vezető
  - Üzemeltetési vezető
  - Egyéb döntéshozók

## Eredmény: egyszerű, gyors és olcsó megoldás

# A megoldás működése



# Automatikus normalizálás

- Az értékes információ kiemelése az adattömegből újra felhasználható módon
- Szabályok készítése
  - intuitív, moduláris, újra felhasználható
  - automatikus felismerés
- Gyors feldolgozás

```
2014-01-23 12:34:12 Conn. from 1.2.3.4 to 3.4.5.6:3232 established.
2014-01-23 12:38:15 Conn. from 1.2.3.4 to 3.4.5.6:3232 closed.
```

| date | time | src_ip | dest_ip | dest_port | type |
|---|---|---|---|---|---|
| 2014-01-23 | 12:34:12 | 1.2.3.4 | 3.4.5.6 | 3232 | open |
| 2014-01-23 | 12:38:15 | 1.2.3.4 | 3.4.5.6 | 3232 | close |

# Számosság alapú súlyozás

```
2021-01-23 12:34:12 Conn. from 1.2.3.4 to 3.4.5.6:3232 estabilished.
2021-01-23 12:34:15 Conn. from 1.2.3.5 to 3.4.5.6:3232 estabilished.
2021-01-23 12:34:19 Conn. from 1.2.3.6 to 3.4.5.6:3232 estabilished.
2021-01-23 12:38:15 Conn. from 1.2.3.4 to 3.4.5.6:3232 closed.
2021-01-23 12:38:15 Conn. from 1.2.3.5 to 3.4.5.6:3232 closed.
2021-01-23 12:38:15 Conn. from 1.2.3.6 to 3.4.5.6:3232 closed.
```

| date | minute | type | dest_ip | dest_port | count |
|---|---|---|---|---|---|
| 2021-01-23 | 12:34 | open | 3.4.5.6 | 3232 | 3 |
| 2021-01-23 | 12:38 | close | 3.4.5.6 | 3232 | 3 |

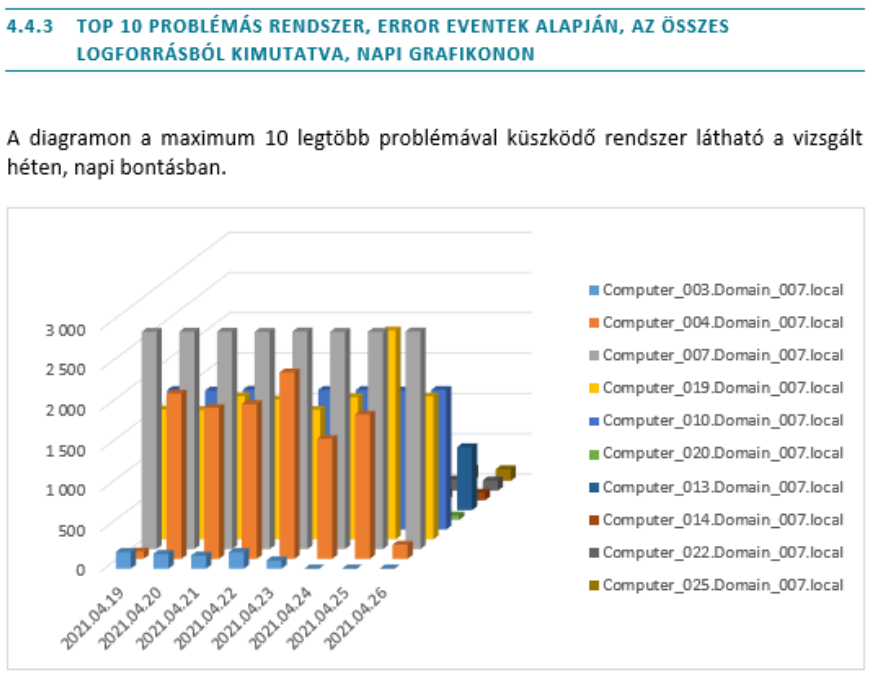
# Számosság alapú statisztikák

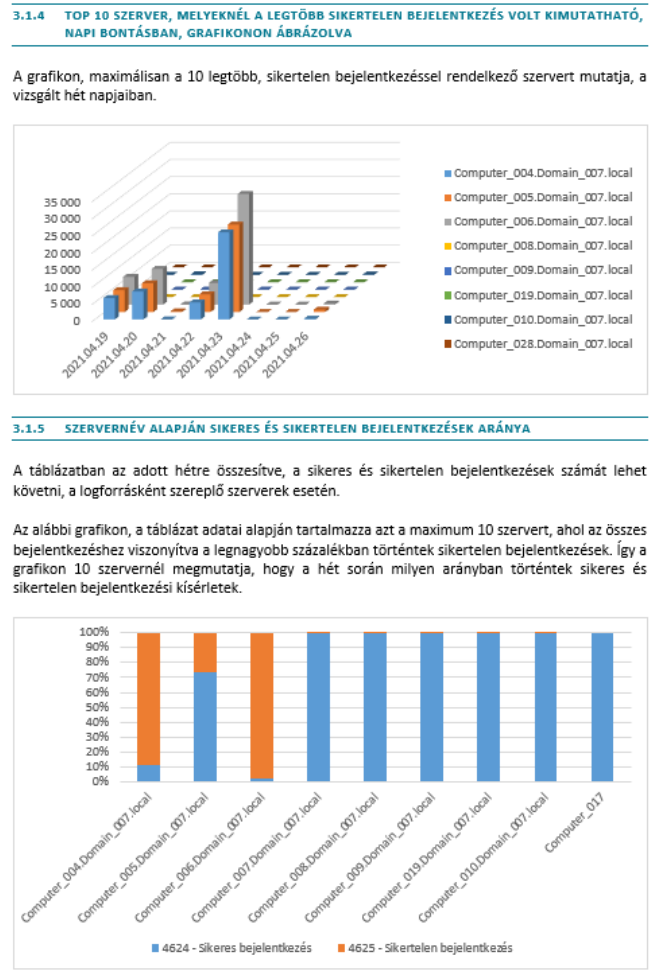
Milyen számosság alapú statisztikák nyerhetők ki a forrásrendszerekből?
Adott időszakban, szerveren vagy kliensen:

- Bejelentkezési események
- Felhasználói fiókok kezelése
- Jogosultságkezelési műveletek
- Naplózással kapcsolatos események
- Rendszerdátummal kapcsolatos események
- Rendszerleállás, újraindítás
- Hardver és szoftver konfigurációváltozás
- Rendszerben fellépő hibák

# Jelentések, következtetések

- Felhasználó
- Időpont
- Kliensgép
- Rendszer
- Kibertámadás
- Szerver
  - Hiba jelentések
  - Alapzaj
  - Üzemeltetési probléma

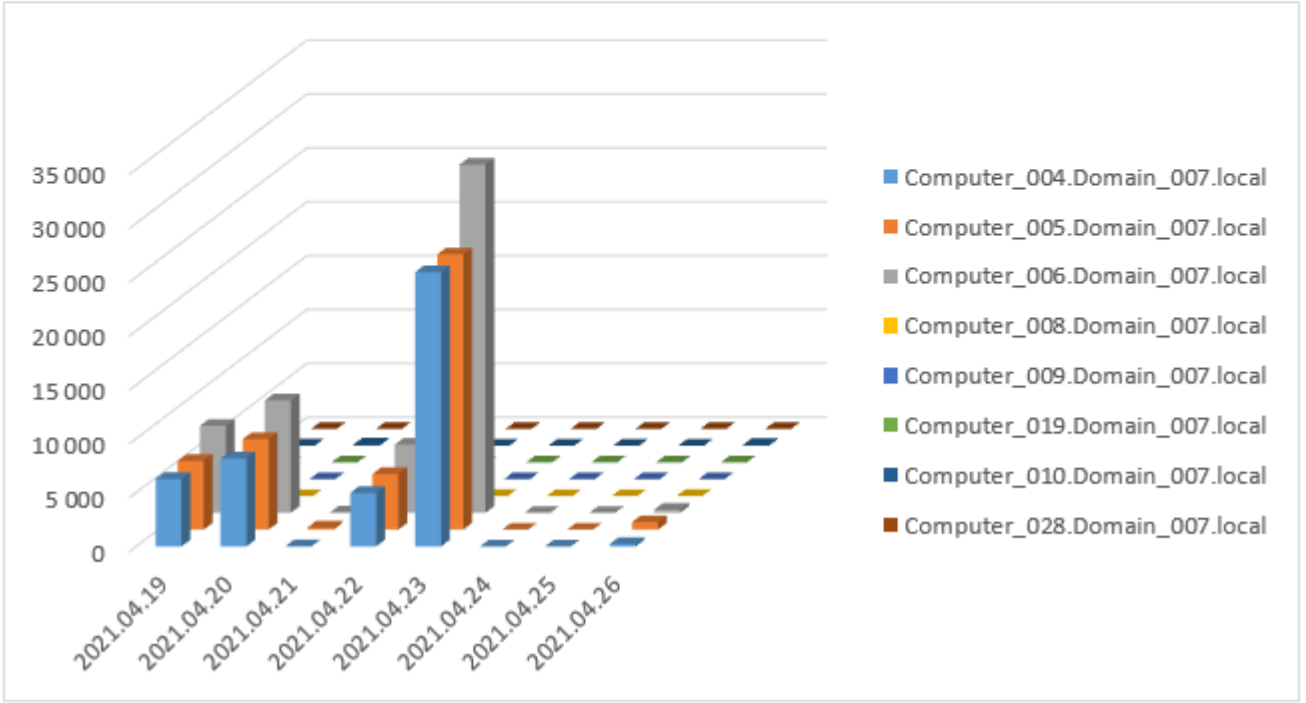


# Grafikonok a jelentéseben

## A grafikonok

- ✓ Megkönnyítik a keresést,
- ✓ Kényelmessé teszik a heti események értékelését,
- ✓ A kiugró viselkedést látványosan ábrázolják,
- ✓ Kiemelik a 10 legproblémásab szervert vagy felhasználót.



# Előnyök a hagyományos adatelemzéshez képest

| | | |
|---|---|---|
| Nem igényel üzemeltetési személyzetet | Nincs szükség adatelemző szakértőkre | Bármely eszköz adattípusának feldolgozása |
| Az adattömegből kiválasztja a fontos információkat | Automatikus heti és havi jelentés generálás | Az ügyfél igényeinek megfelelő finomhangolhatóság |
| Központi adattárház nélküli működés | A rendszerekben végbemenő biztonsági folyamatok, trendek bemutatása | Biztonsági döntések alátámasztása |

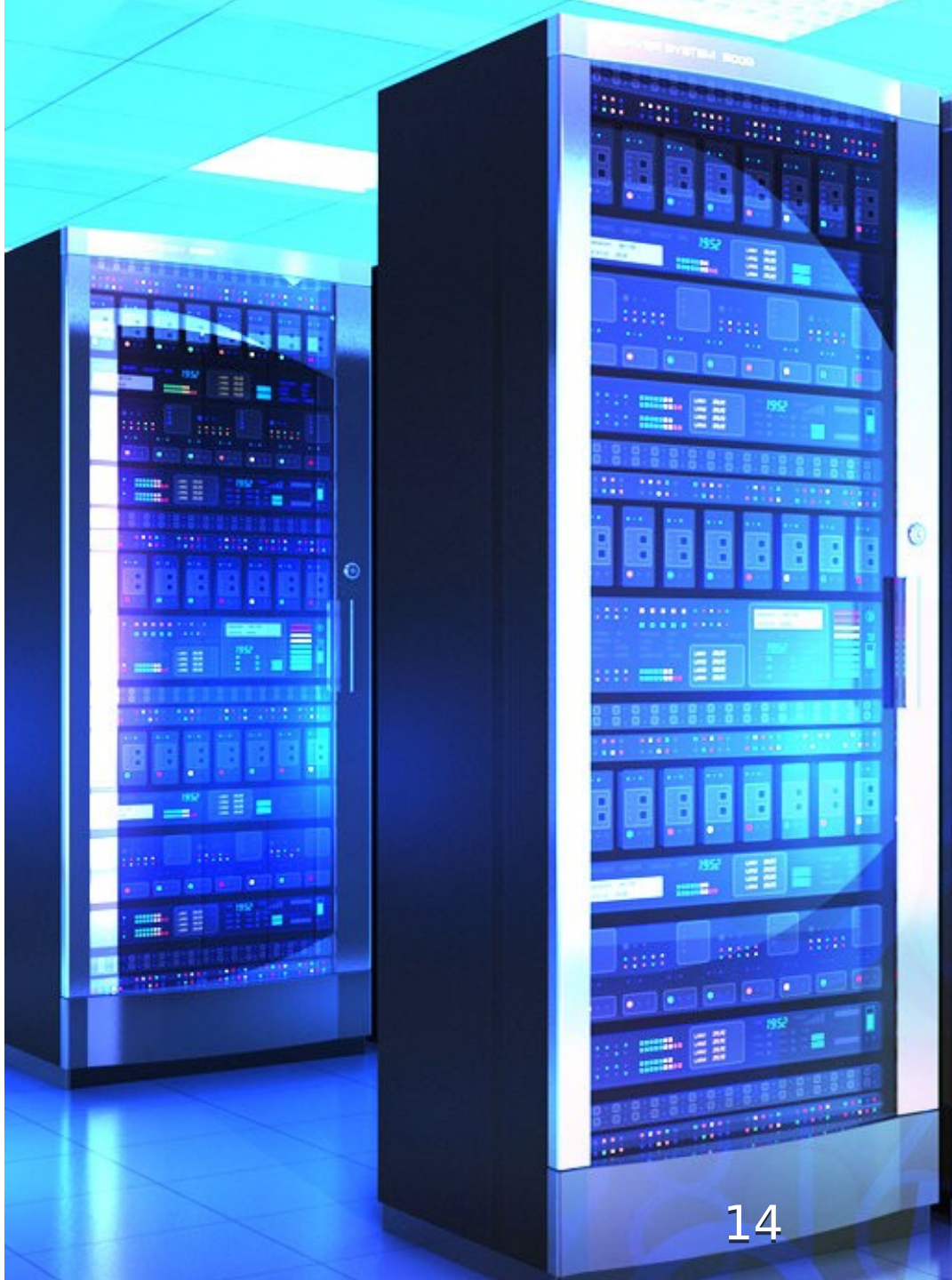
# Innovációs irányok

## Adattárolás, archiválás

- ✓ Nagy tárkapacitás
- ✓ Időpecsét
- ✓ Titkosított adatok
- ✓ Mély szintű nyomozás lehetősége

## Intelligens monitorozás

- ✓ Trendelemzés
- ✓ Forecasting
- ✓ Esemény előtti riasztás küldése
- ✓ Proaktív beavatkozás a működésbe



# GONDOLKODJ KOMPLEXEN, **CSINÁLD EGYSZERŰEN.**

**Kótai Szabolcs**
**SeConical termékmenedzser**
***IT GRC szakértő***

seconical@kurt.hu
www.seconical.hu