eCSI

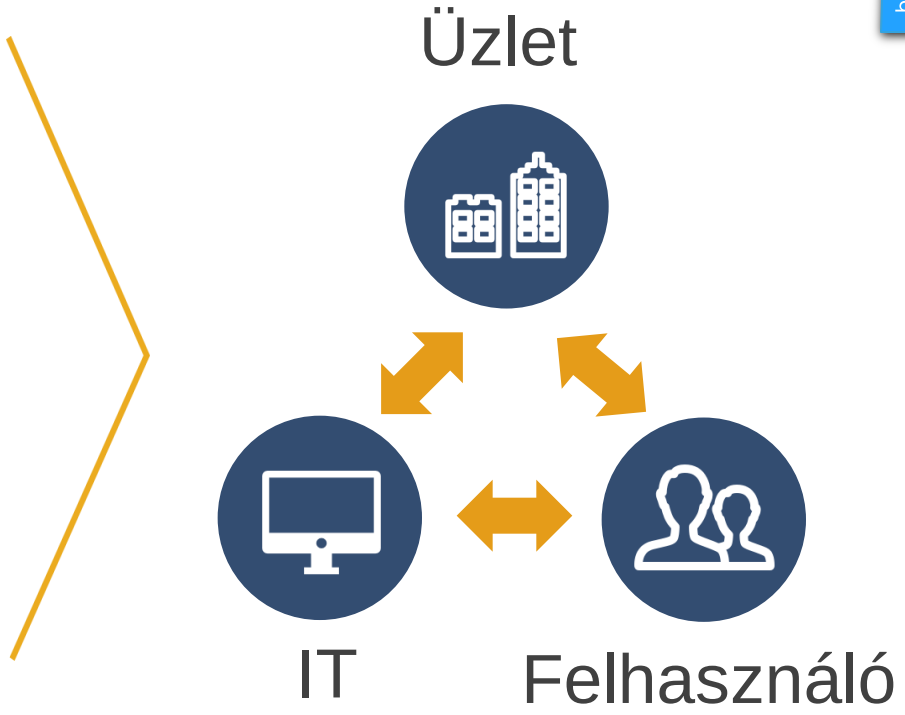
Felhasználóbarát IT biztonság

balabit.com

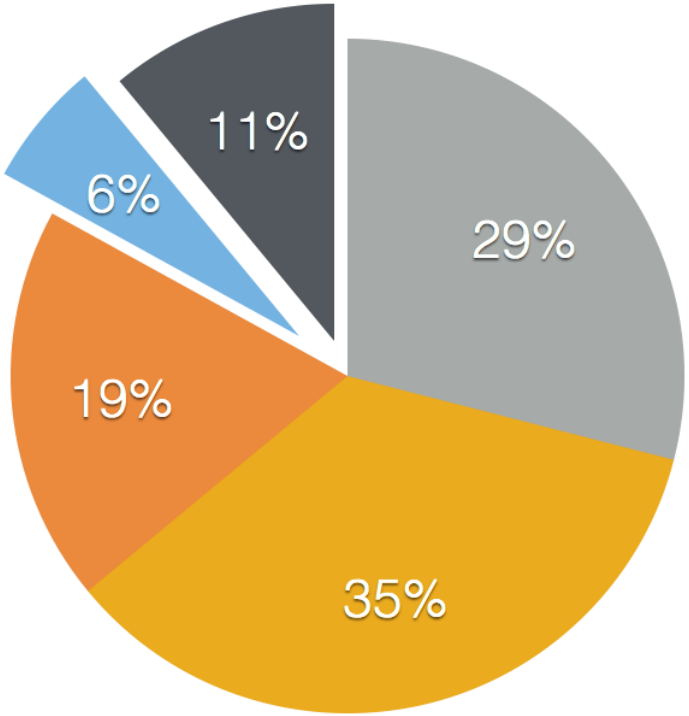
CRIME SCENE eCSI OFFICERS ONLY

Minden megváltozott

- Mobil
- Felhő
- Social
- Consumerization



Tények



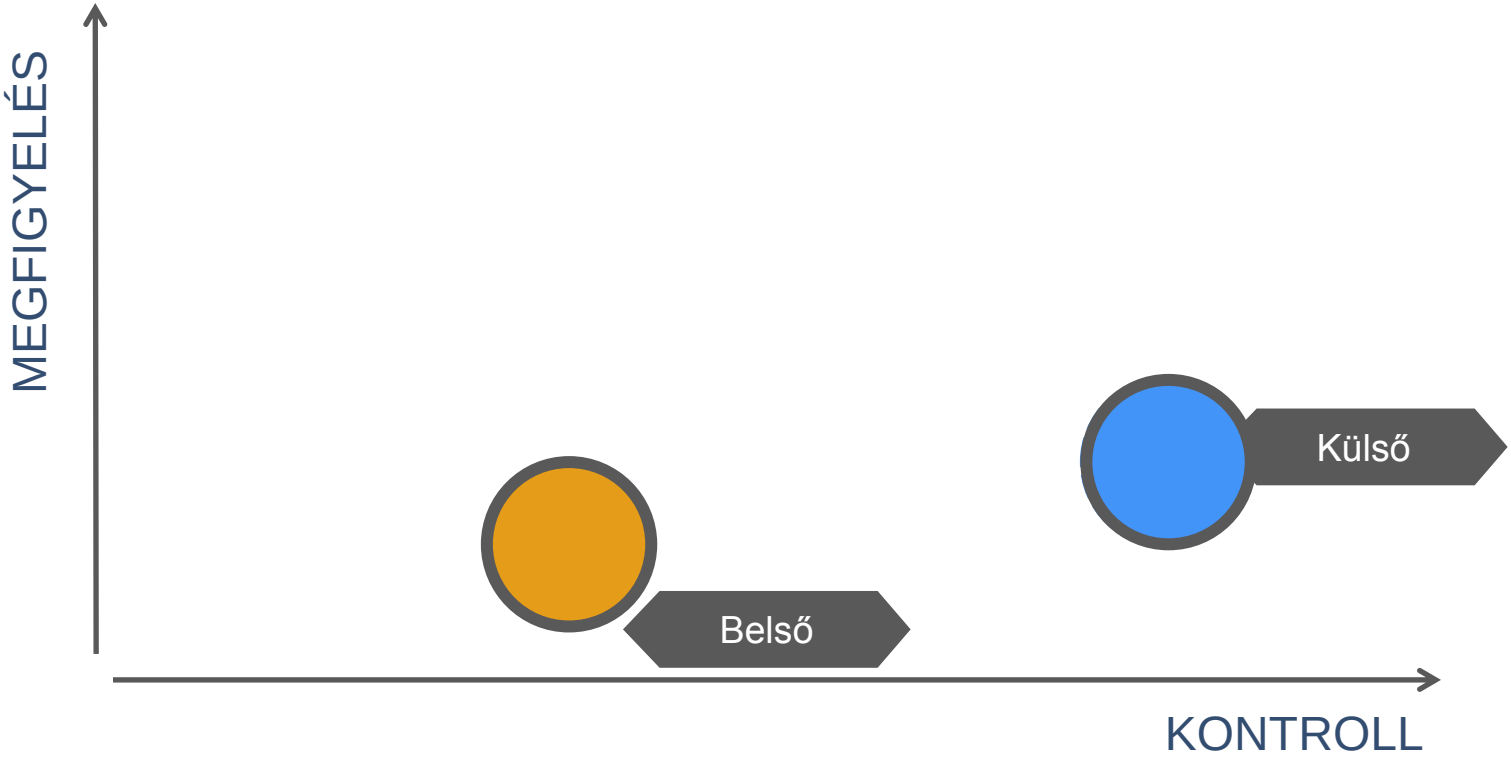
- Hibás működés
- Emberi mulasztás
- Belső elkövető
- Külső elkövető
- Automatizált támadás

60% Ember

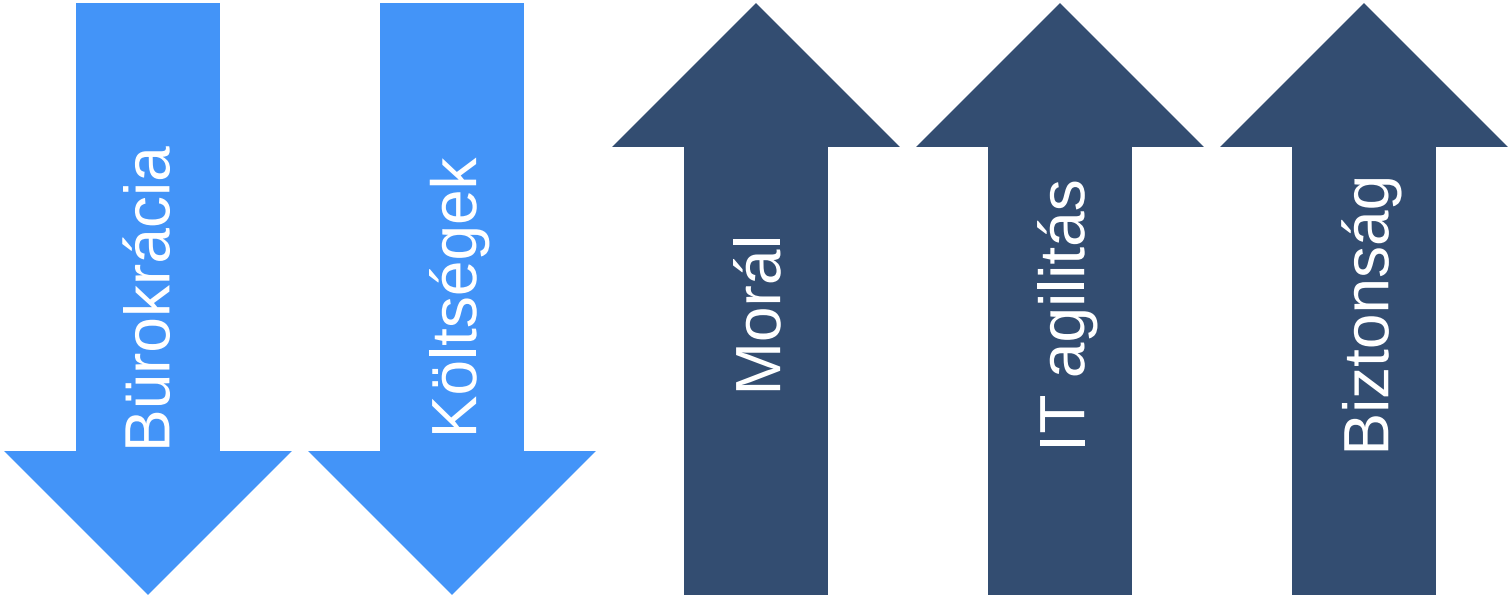
54% Belső

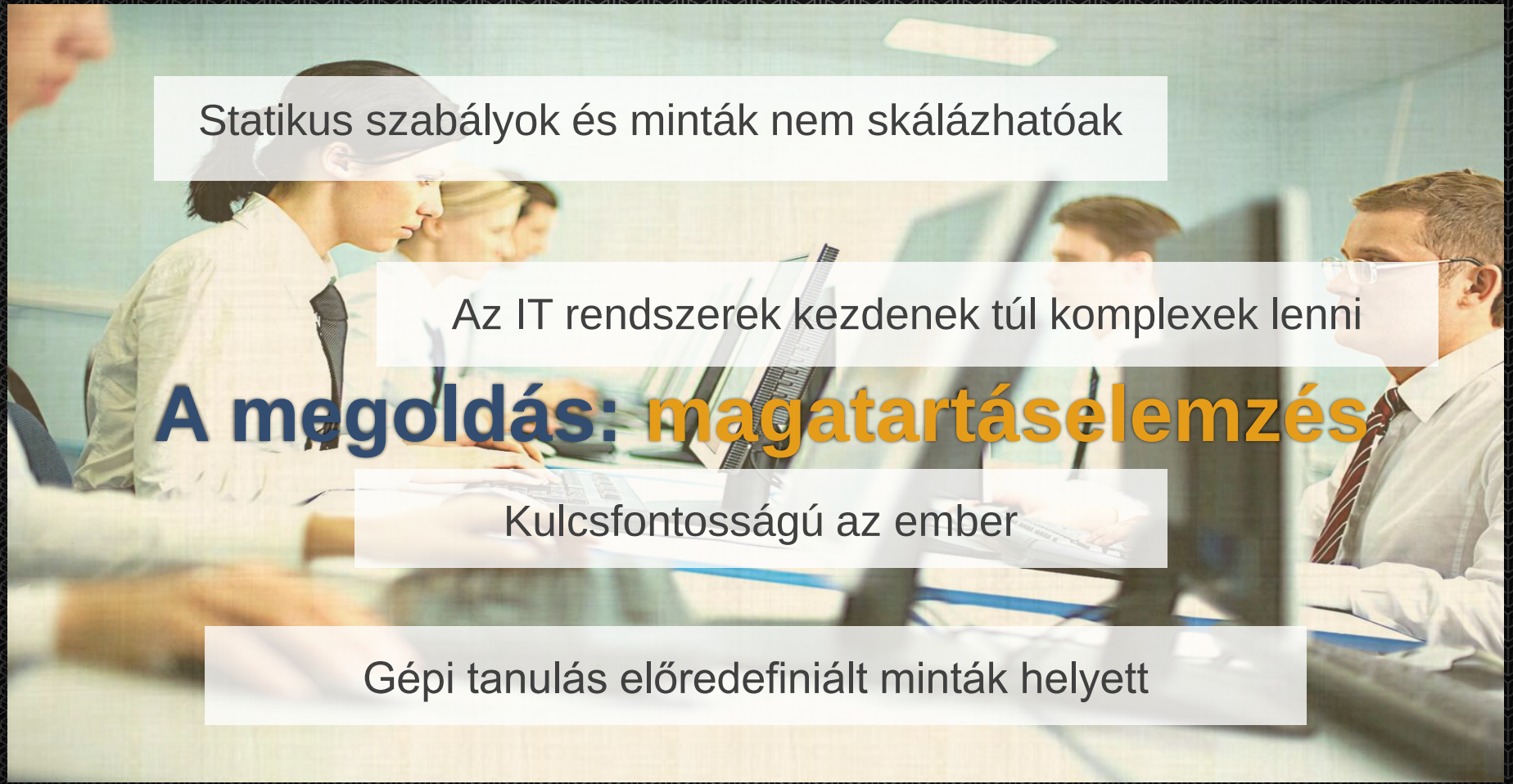
Source: Ponemon, 2013

Hol van a hangsúly a fenyegetés kontrollban?



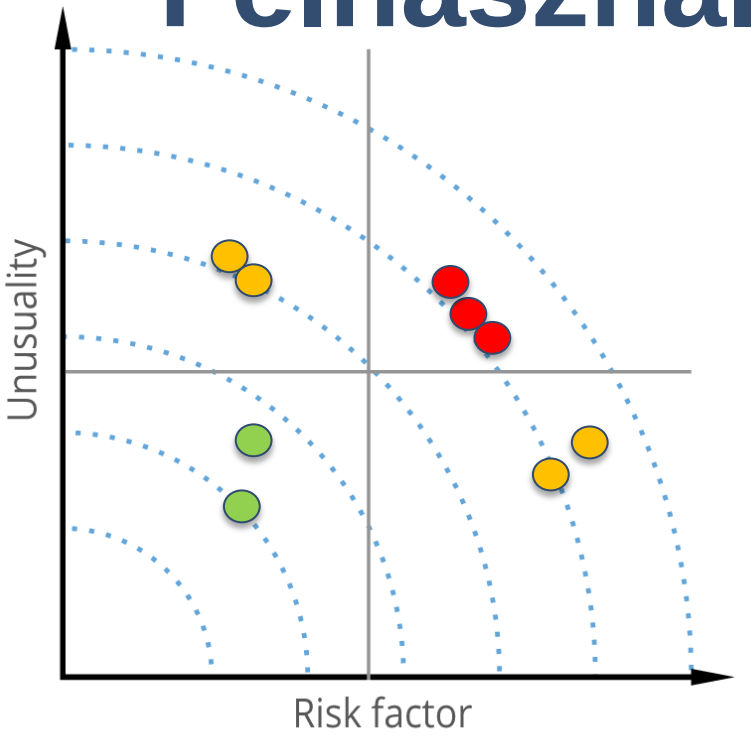
A megfigyelésközpontúság előnyei




Statikus szabályok és minták nem skálázhatóak
Az IT rendszerek kezdenek túl komplexek lenni
A megoldás: magatartáselemzés
Kulcsfontosságú az ember
Gépi tanulás előredefiniált minták helyett

Felhasználóanalízis

Felhasználó és kockázat



Priority list

event #43
event #22
event #14

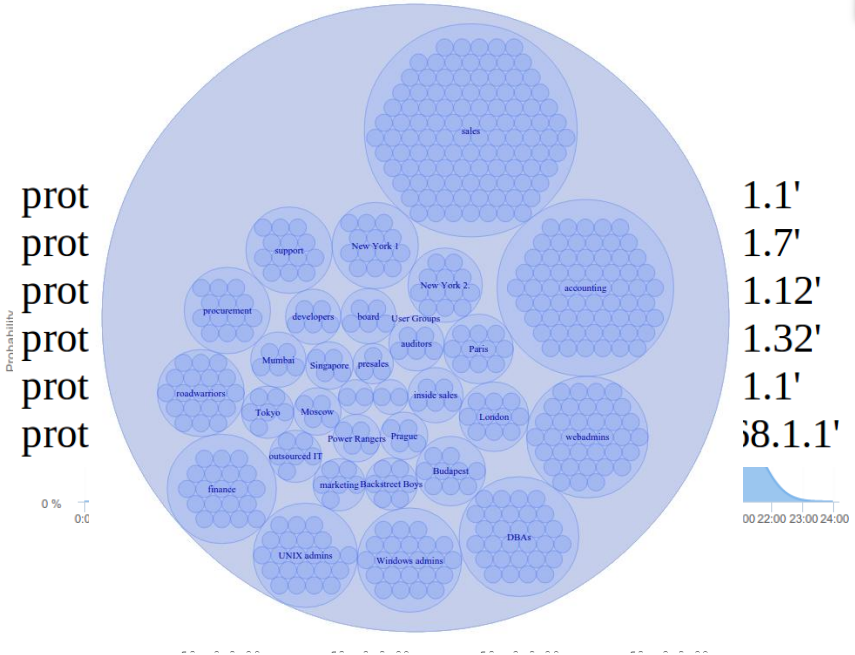
event #12
event #34
event #27
event #10

event #40
event #22
event #18

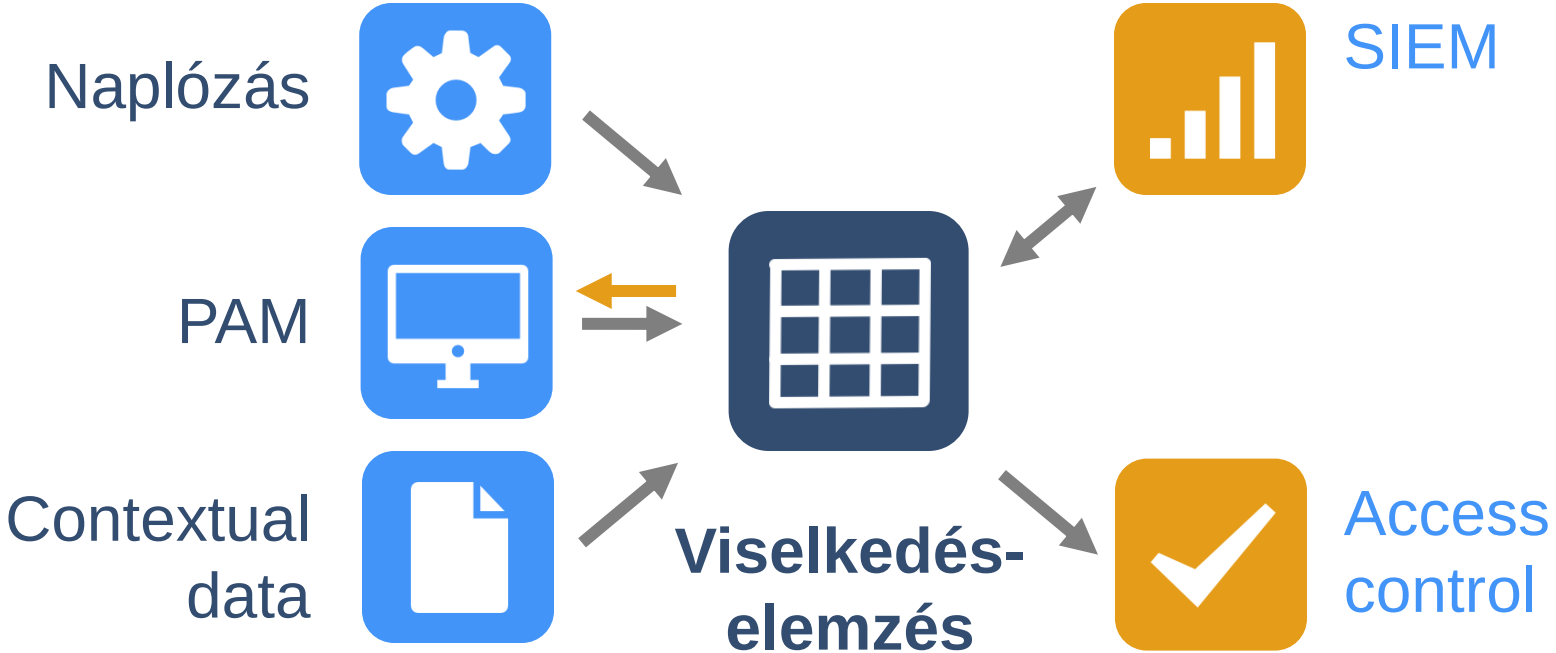
balabit.com

Matematikai háttér

- Nincs egy csodaalgoritmus
  - időeloszlások
  - automatizált mintakeresés
  - ajánlórendszerek
  - szöveganalízis



Contextual Security Intelligence



BalaBit eCSI-portfólió

balabit.com

Blindspotter

- Viselkedéselemzés
- Valósidejű dashboardok
- Priorizált listák
- Környezet megmutatása
- Automatikus reakció
- Érzékeny adatok védve

Syslog-ng

- Megbízható naplózás
- Sokféle adatforrás
- Magas teljesítmény

Shell Control Box

- Független adatforrás
- Részletes felvétel
- Kontrollpont

Kérdések?