BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Data science az IT biztonságban

Windhager-Pokol Eszter

I. Eduárd angol király

BALABIT

SIEM

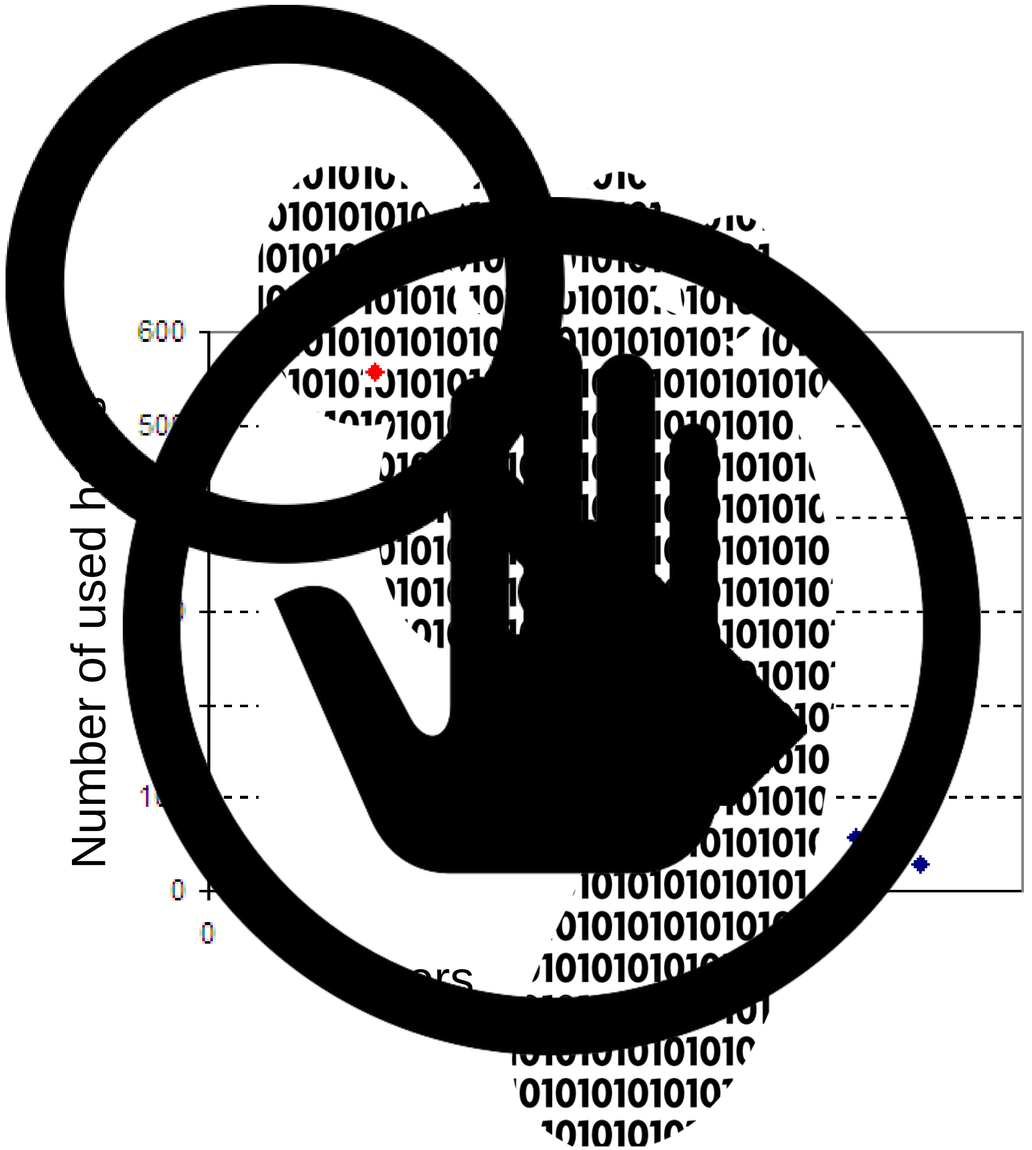
Rögzített szabályok

- Nagy kihívás a szabályrendszert felállítani
  - Felhasználók korlátozása
  - Adatokkal való visszaélés megelőzése
- Karbantartás szinte lehetetlen
  - A környezet és a felhasználók szerepköre folyamatosan változik
- **Csak ismert támadások ellen véd**

BALABIT

Blindspotter

- Összegyűjti a userek digitális lábnyomát
- Elkészíti a baseline-t „normális” viselkedésről
- Azonosítja a szokatlan aktivitásokat valós időben
- Azonnali reakció az adatokkal való visszaélés megelőzéséhez



BALABIT

Példa

BALABIT

Döntéshozásra jutó idő

BALABIT

User Behavior Analysis

Egydimeziós

- **Login Time**
- **Command elemzés**
- **Recommender system**
- **Window title elemzés**
- **Aktivitások száma**

Többdimenziós

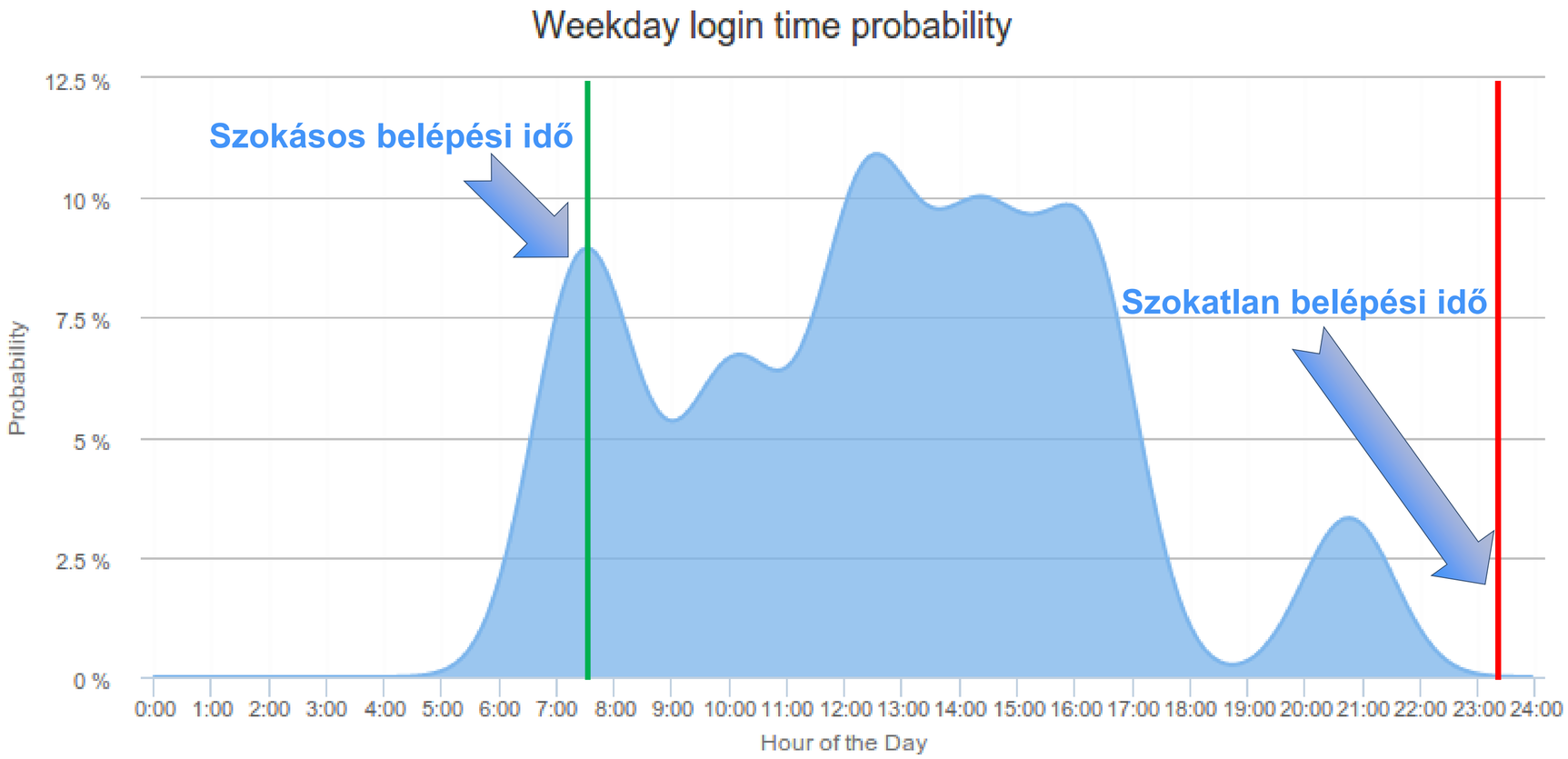
- **Frequent ItemSet**
- **Principal Components Classifier**

Biometrikus azonosítás

- **Gépelési dinamika**
- **Egérmozgás elemzés**
  - Pointing device azonosítás
  - User azonosítás

BALABIT

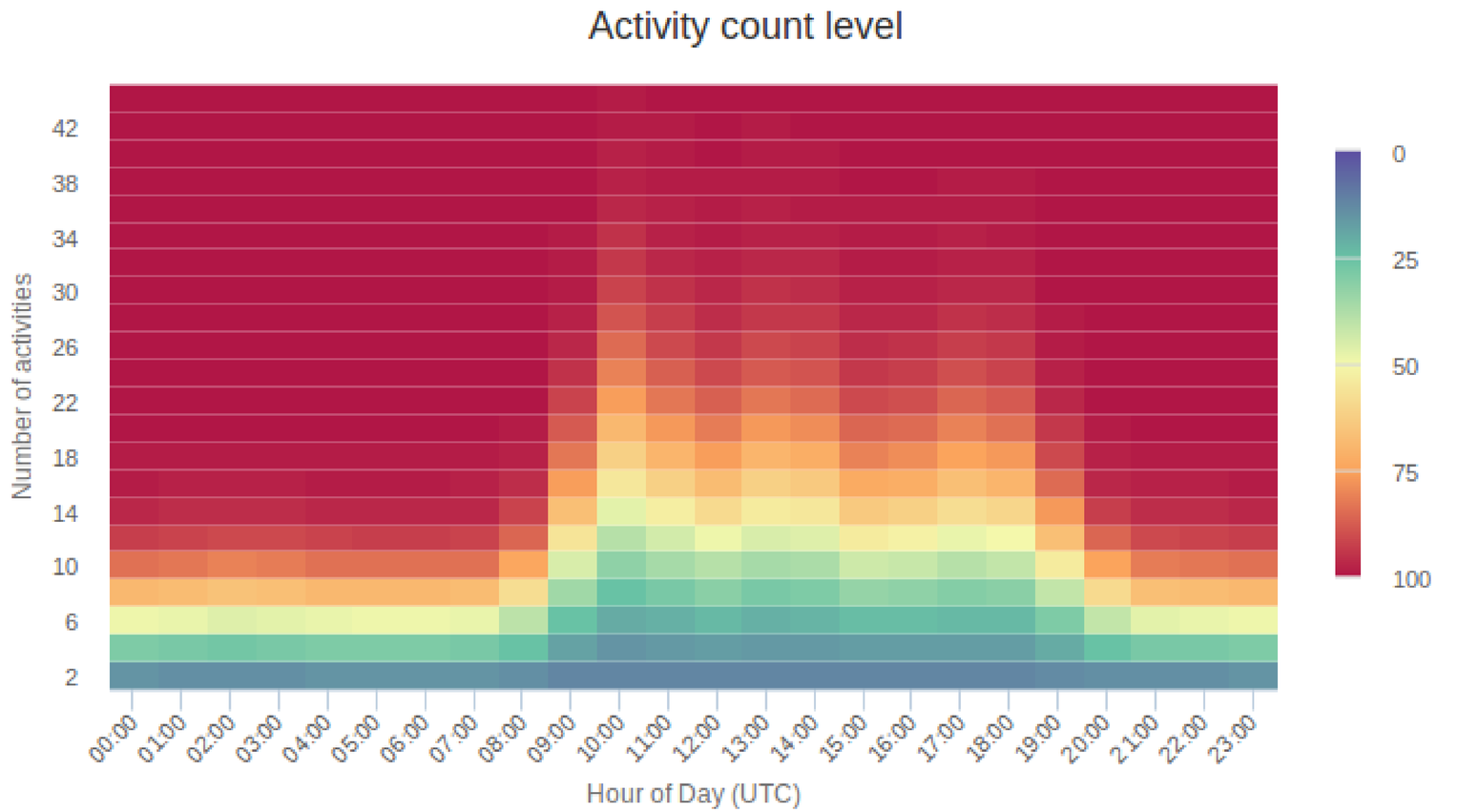
Logintime distribution



BALABIT

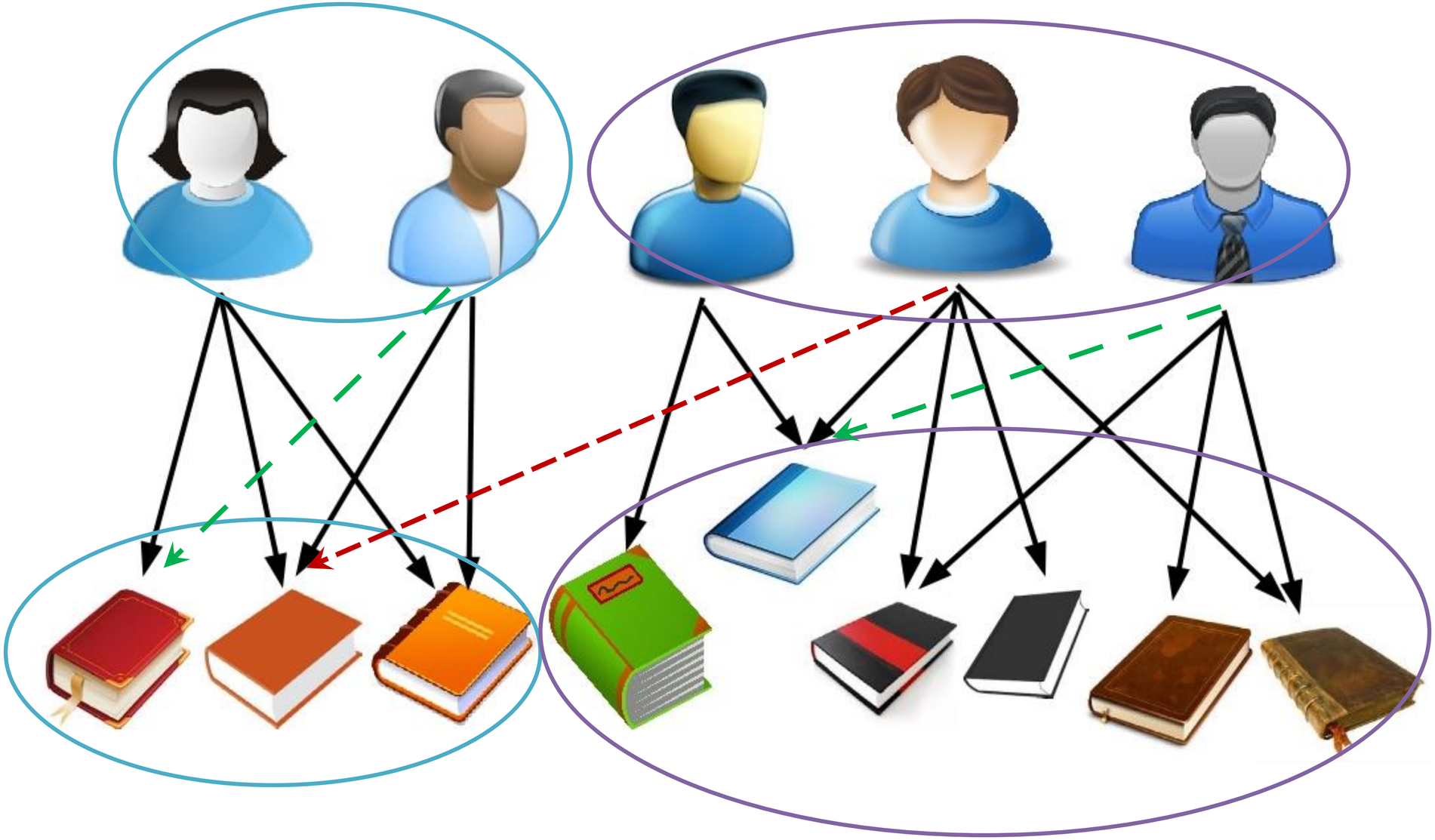
Activity count

Aktivitások szokásos száma időszakonként



BALABIT

Ajánlórendszerek



BALABIT

Frequent ItemSet

Gyakori mintázatok keresése

start_time_is_workday	**true**

start_time_is_workday	**true**	auth_method	**0**	protocol	**rdp**	src_ip	**209.156.29.226**	port	**3389**

start_time_hour	**8-13**	start_time_is_workday	**true**

channels->verdict.ACCEPT	**true**	start_time_is_workday	**true**

auth_method	**0**	start_time_is_workday	**true**	start_time_hour	**8-13**	src_ip	**209.156.29.226**	port	**3389**	protocol	**rdp**

BALABIT

Többlépcsős azonosítás

BALABIT

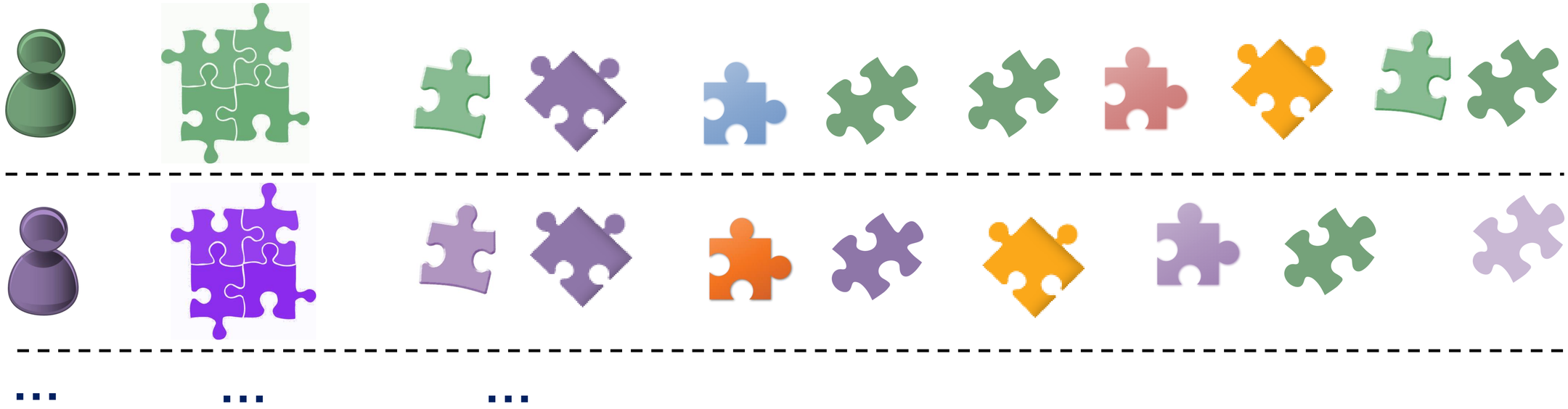
Biometrikus azonosítás

- **Pointing device** azonosítás
  - Mouse
  - Touchpad
- User azonosítása **egérmozgatás** alapján
- User azonosítása **gépelési dinamika** alapján

BALABIT

Modellek kiértékelése

1. Build baseline **2. Future activities** **+ 3. Fake activities**



4. Score activities

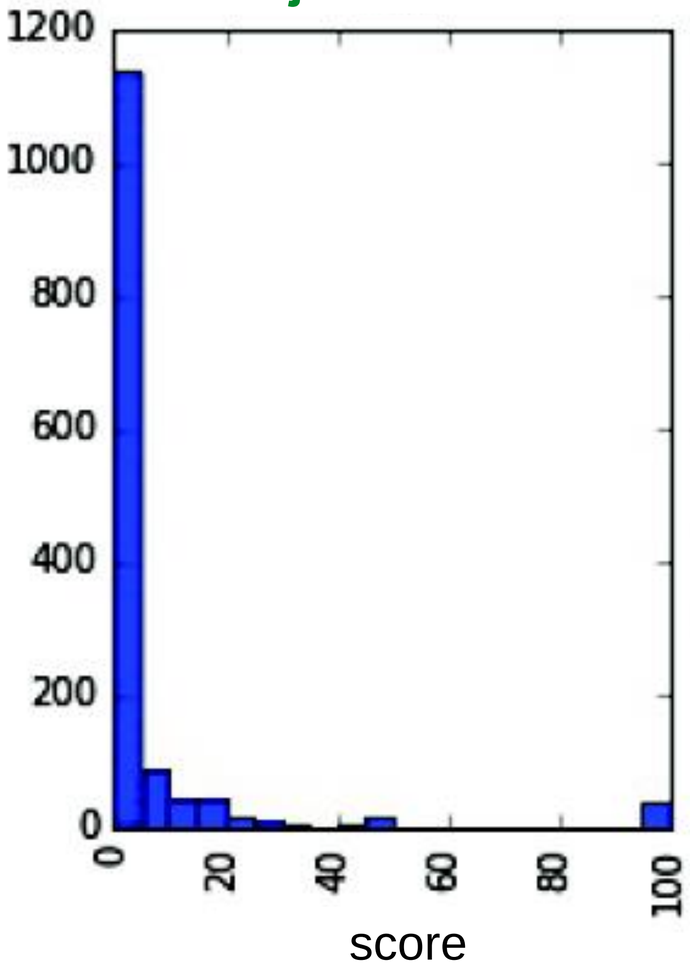
5. Calculate AUC

(Area Under the ROC curve)

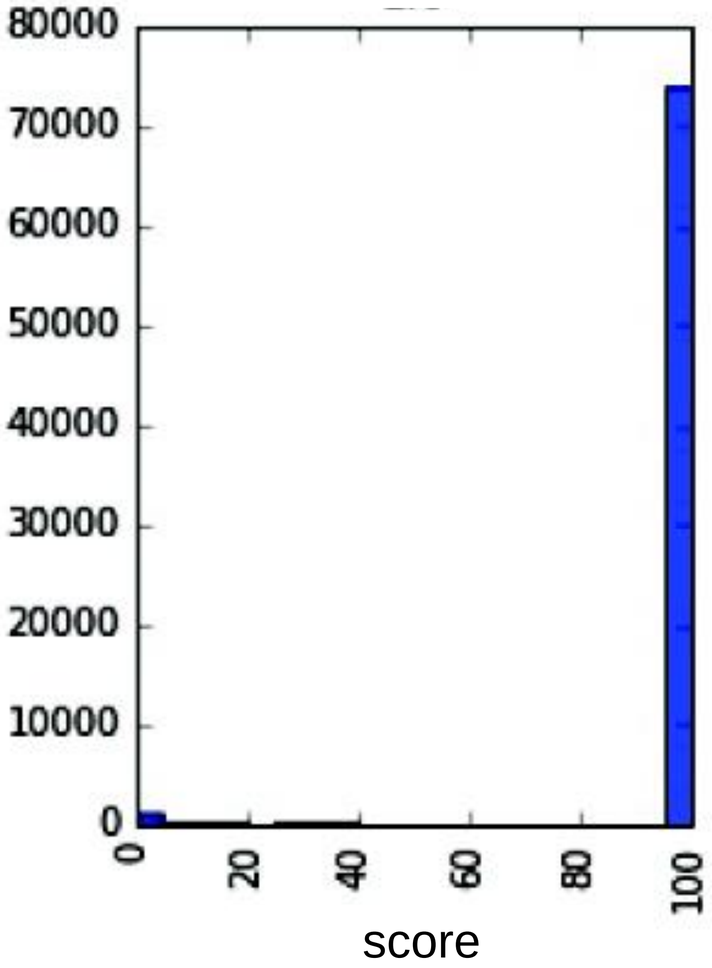
BALABIT

Kiértékelés I.

Saját baseline

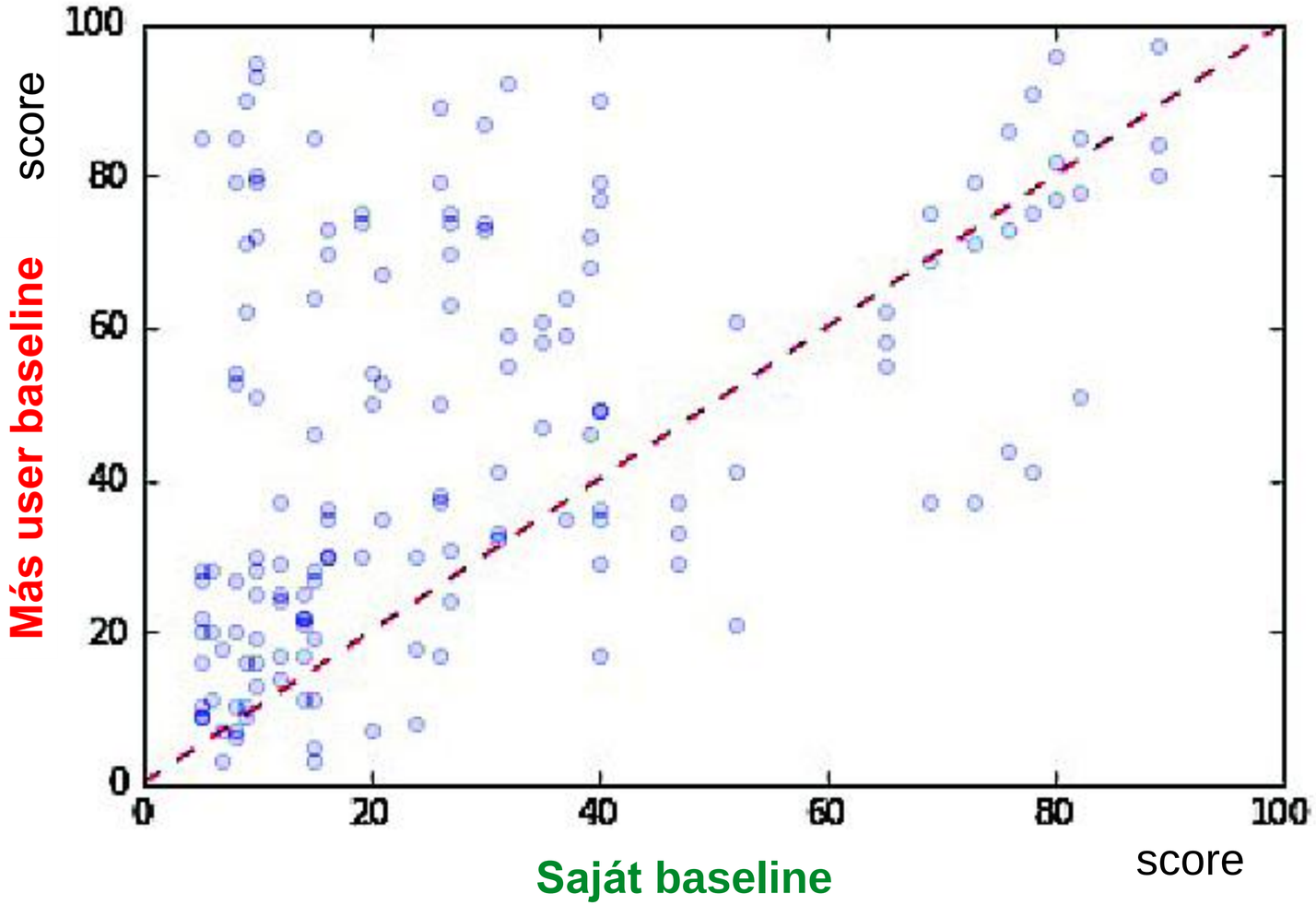


Más user baseline



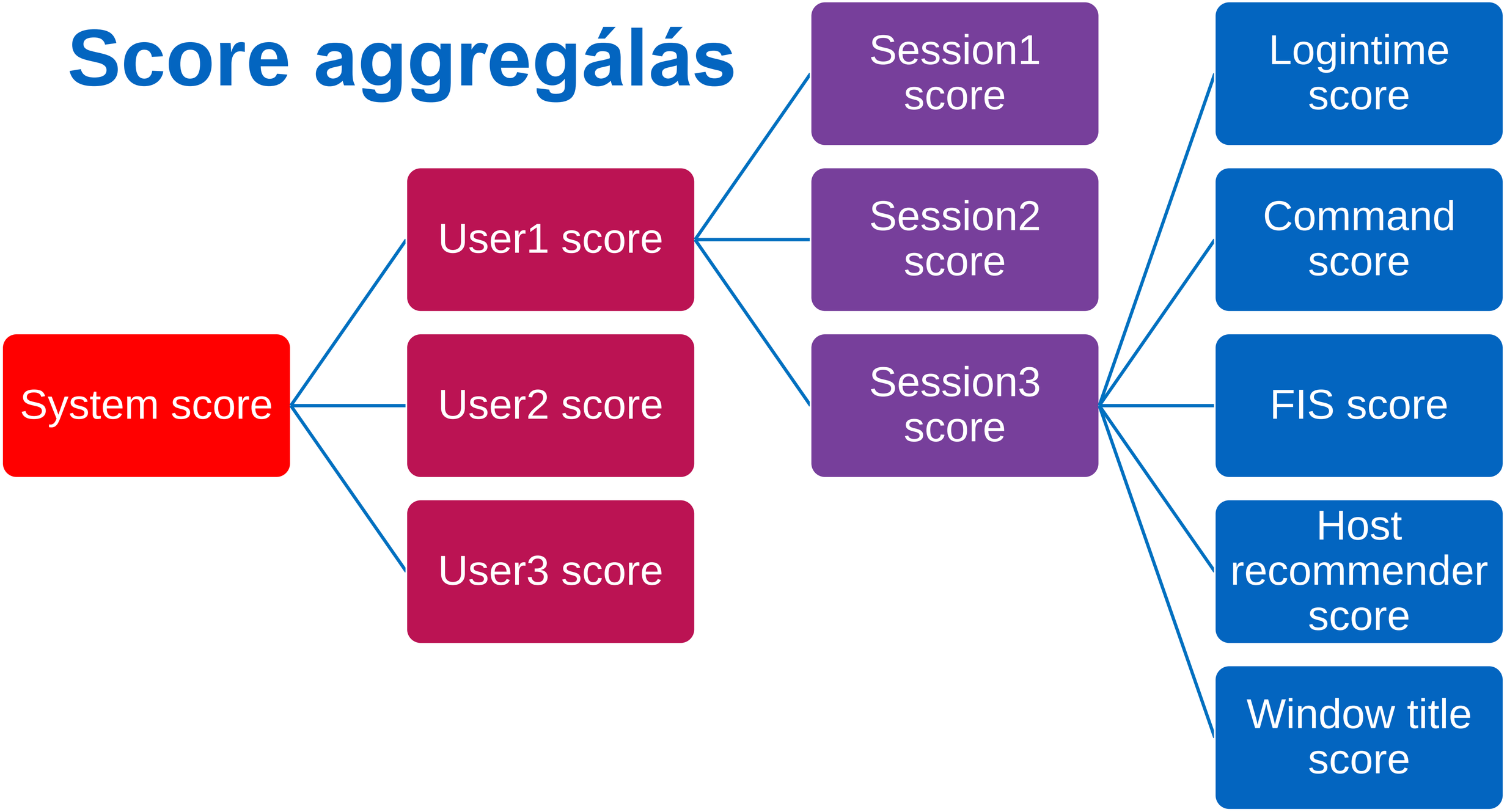
BALABIT

Kiértékelés II.



BALABIT

Score aggregálás

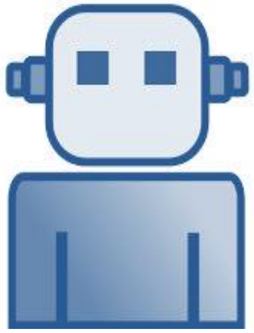


További analitikák

User risk

Peer group

Script detection



BALABIT

User risk

z-score



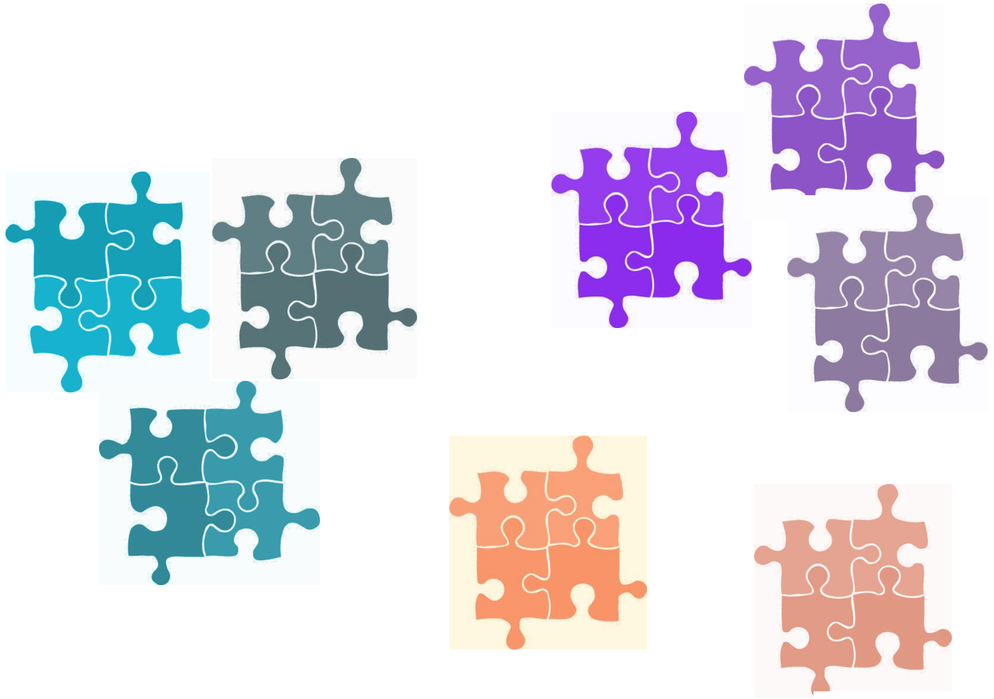
	X	X	...	X
	√	X		X
	√	√		X
	√	√		X
...	...	...		...
	√	√		√

BALABIT

Peer group elemzés

Saját viselkedéshez viszonyítunk

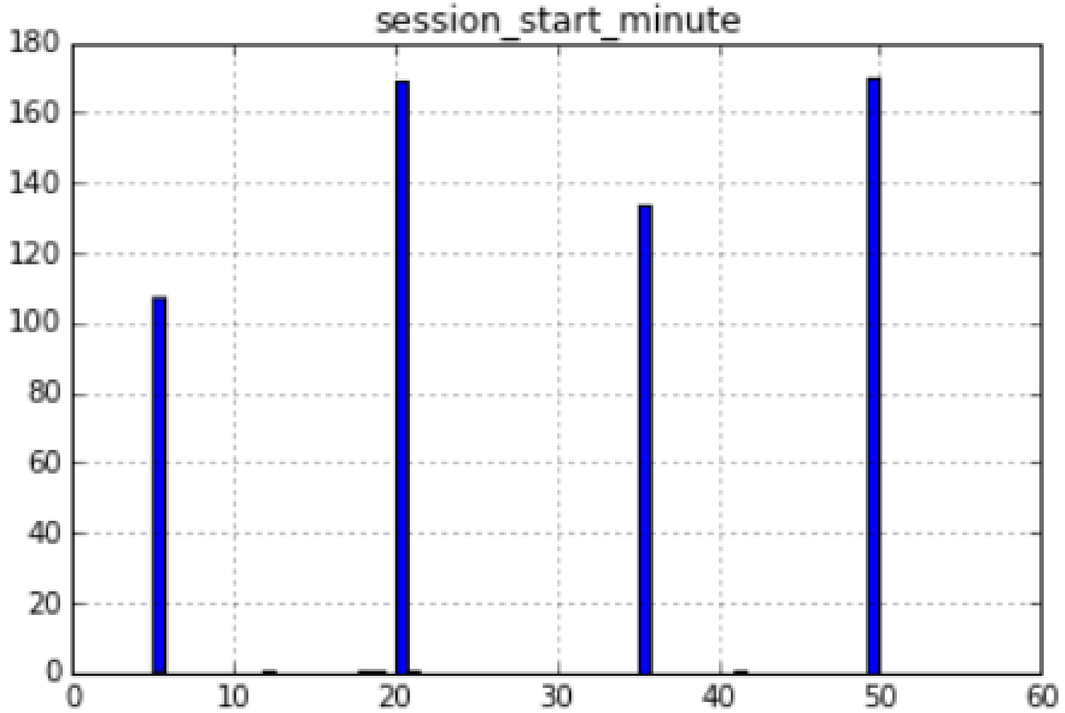
Hasonló userekhez viszonyítunk

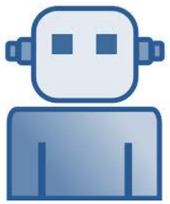


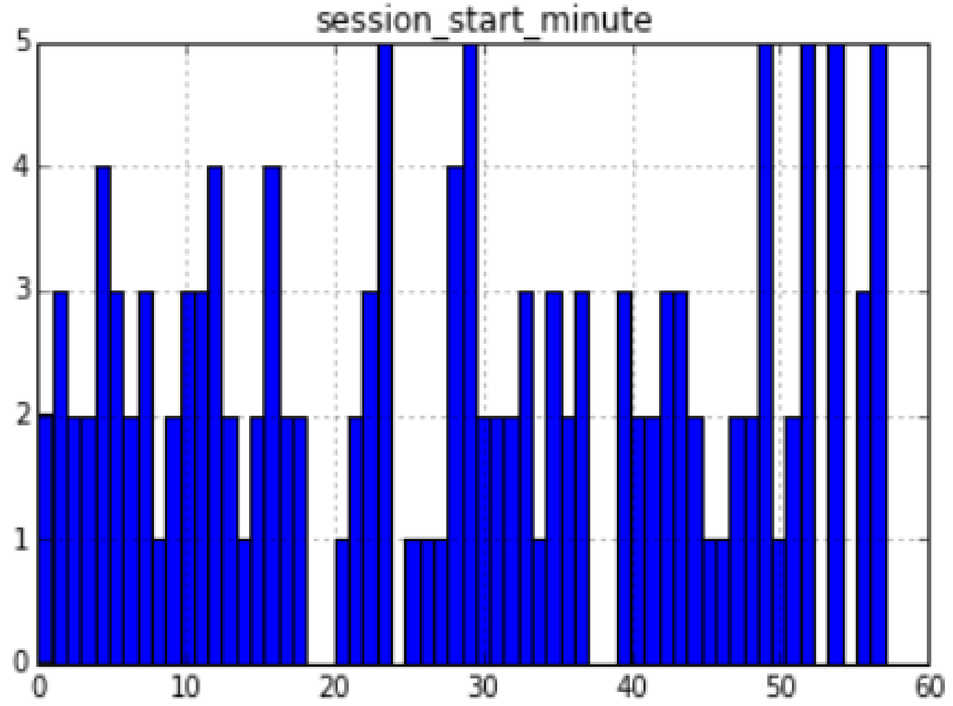
BALABIT

Robotok azonosítása

Ember vagy script?







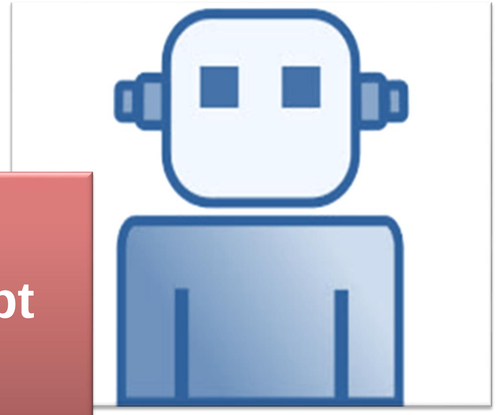
BALABIT

Összefoglalás

Változás

Outlier

Script



Kockáza-
tos user

BALABIT

Kérdések?

eszter.windhager-pokol@balabit.com

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE