



***Az autentikáció egyetlen kérdése, hogy a monitor előtt ülő személy valóban az-e, akinek állítja magát.***



**BALABIT**  
CONTEXTUAL SECURITY INTELLIGENCE

# A biometrikus autentikáció új módszerei

Windhager-Pokol Eszter – senior data scientist

# AGENDA

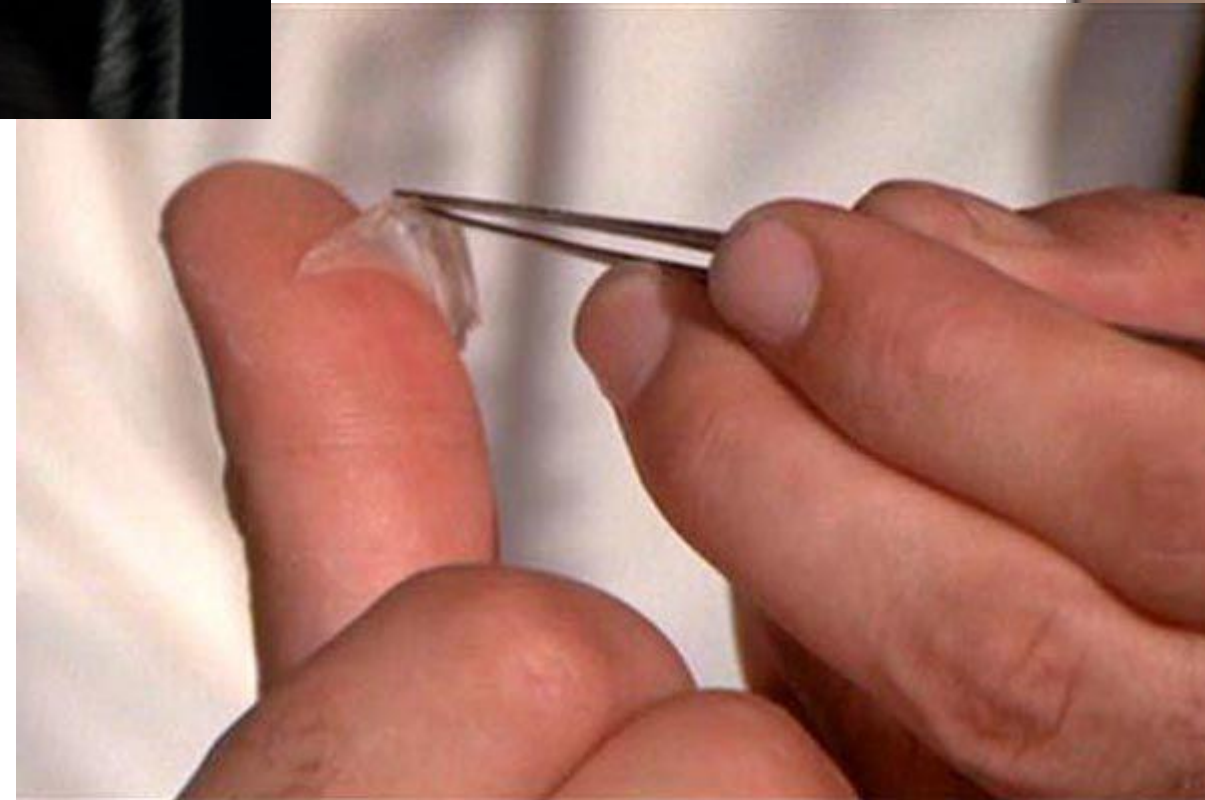
- Autentikációs módszerek
- Biometrikus azonosítás
- További lehetőségek

# AZONOSÍTÁSI MÓDSZEREK FILMEKBEN

**A pusztító: írisz szkener**



**Gattaca:**  
ujjlenyomat olvasó és DNS vizsgálat



**Gyémántok az örökkévalóságnak:**  
ujjlenyomat olvasó

# AUTENTIKÁCIÓS MÓDSZEREK

## Tudás

- Jelszó
- PIN kód
- Személyes adatok

## Birtoklás

- Belépő kártya
- Kulcs
- Mobiltelefon (SMS)

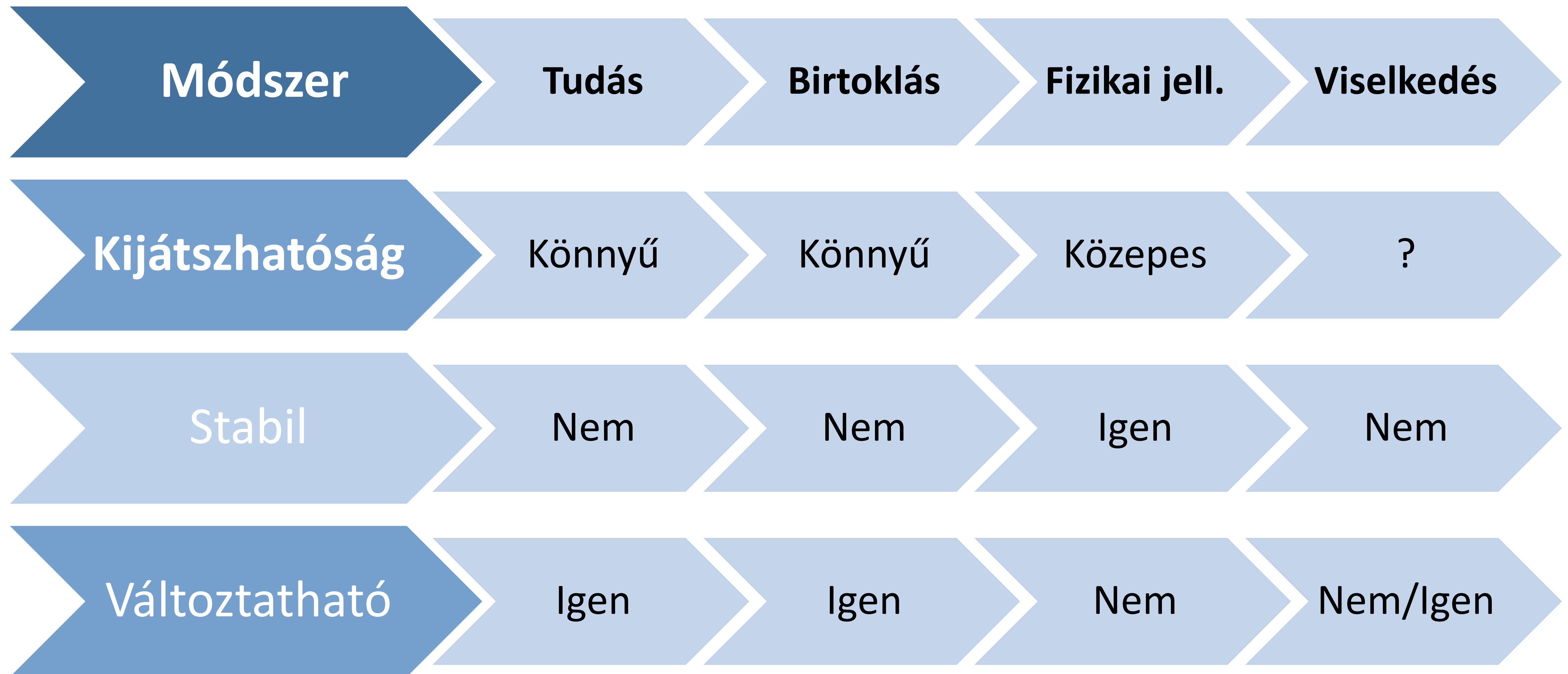
## Fizikai jellemzők

- Ujjlenyomat
- Arc
- Retina
- Véna
- Hang

## Viselkedés

- Egér mozgató
- Gépelési dinamika
- Járás

# ELŐNYÖK ÉS HÁTRÁNYOK



# **VISELKEDÉS ALAPÚ AZONOSÍTÁSI MÓDSZEREK**

## Egér mozgató



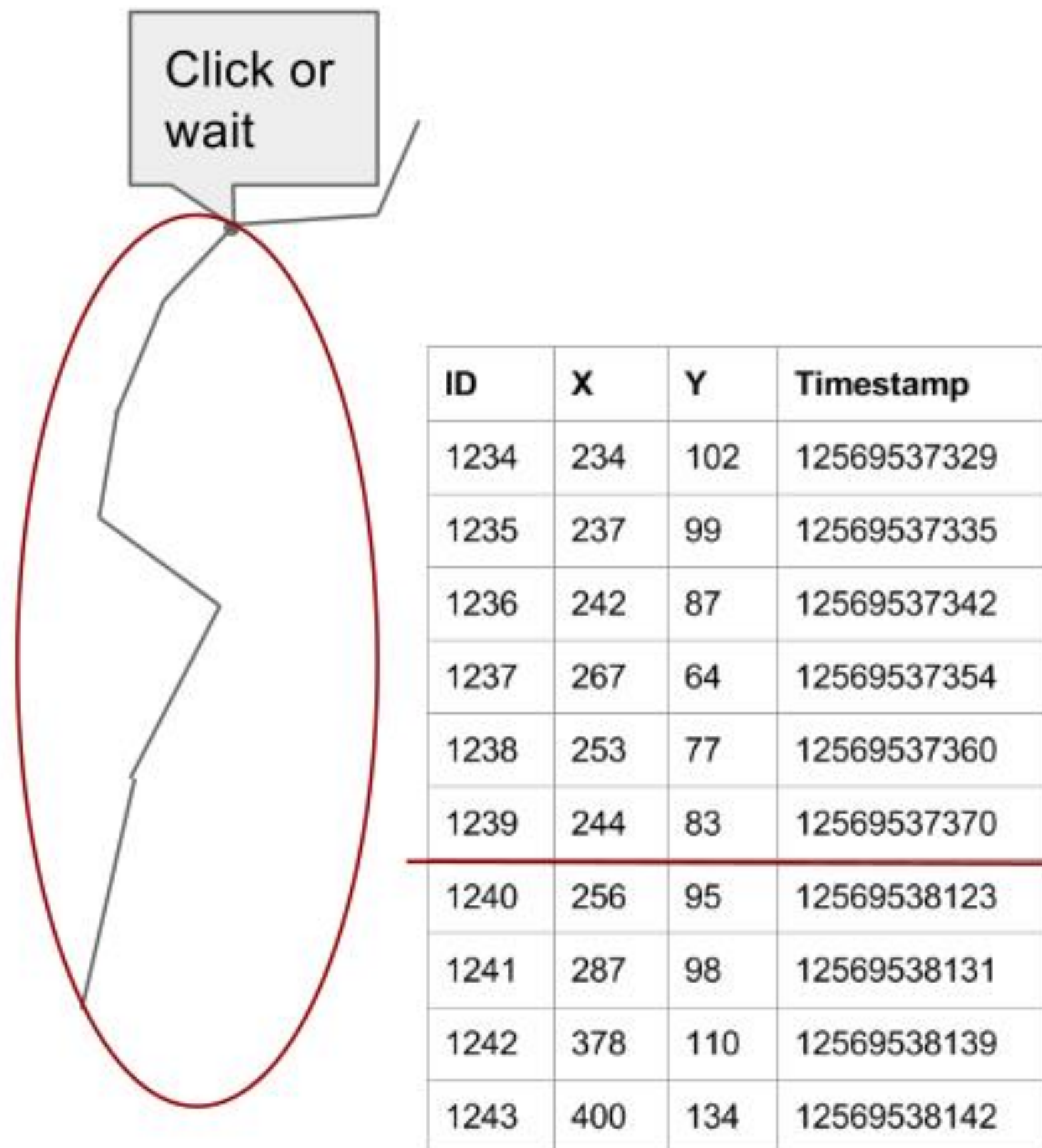
## Gépelés





# Egér mozgás – adatelőkészítés

## Darabolás



## Mozgás jellemzői

ID	X	Y	Timestamp	speed	curvature	...
1234	234	102	12569537329			
1235	237	99	12569537335			
1236	242	87	12569537342			
1237	267	64	12569537354			
1238	253	77	12569537360			
1239	244	83	12569537370			
1240	256	95	12569538123			
1241	287	98	12569538131			
1242	378	110	12569538139			
1243	400	134	12569538142			

## Aggregálás

Movement_ID	speed_min	speed_max	straightness_mean	...
001				
002				
003				
004				
005				
006				
...				

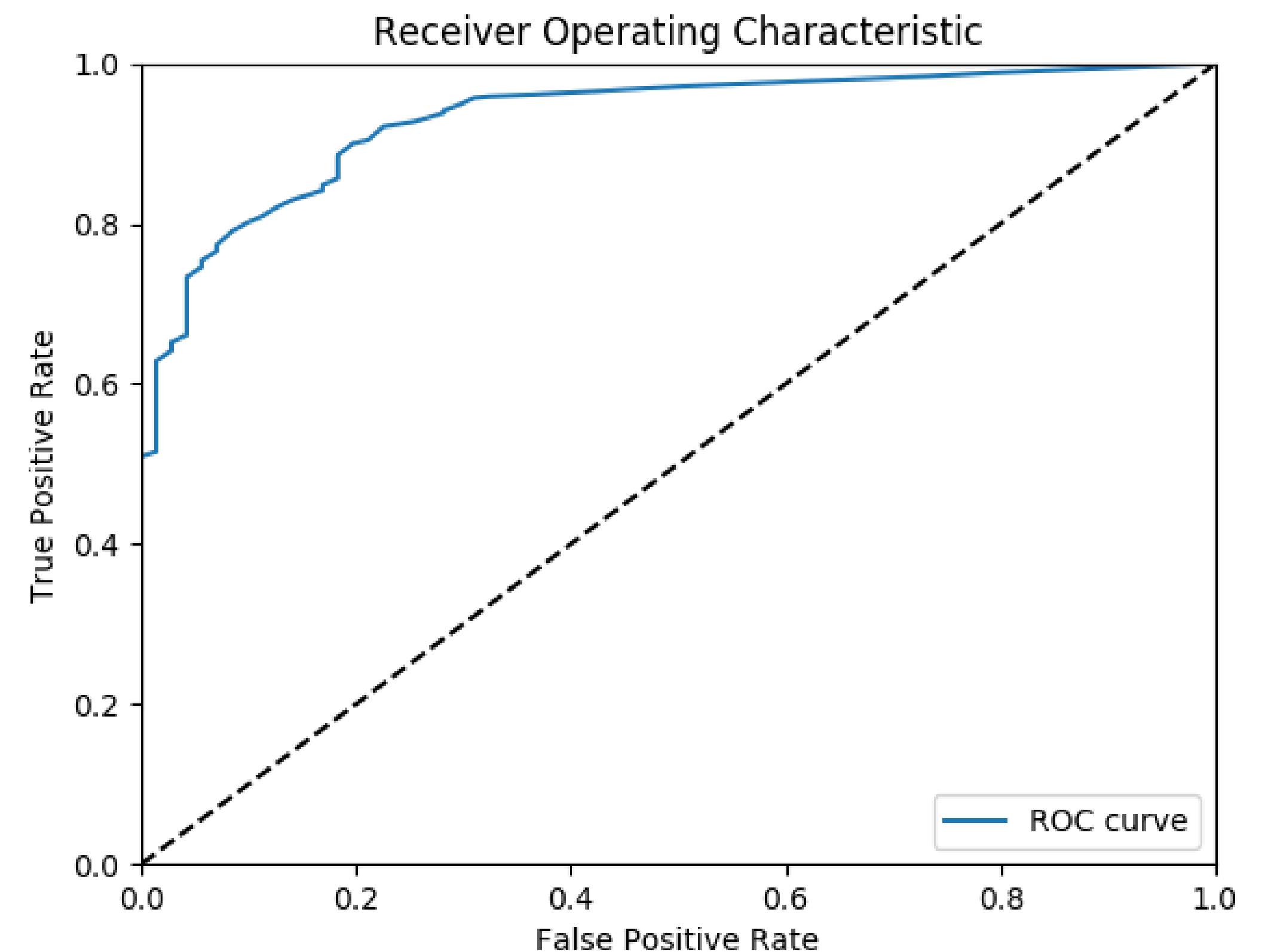
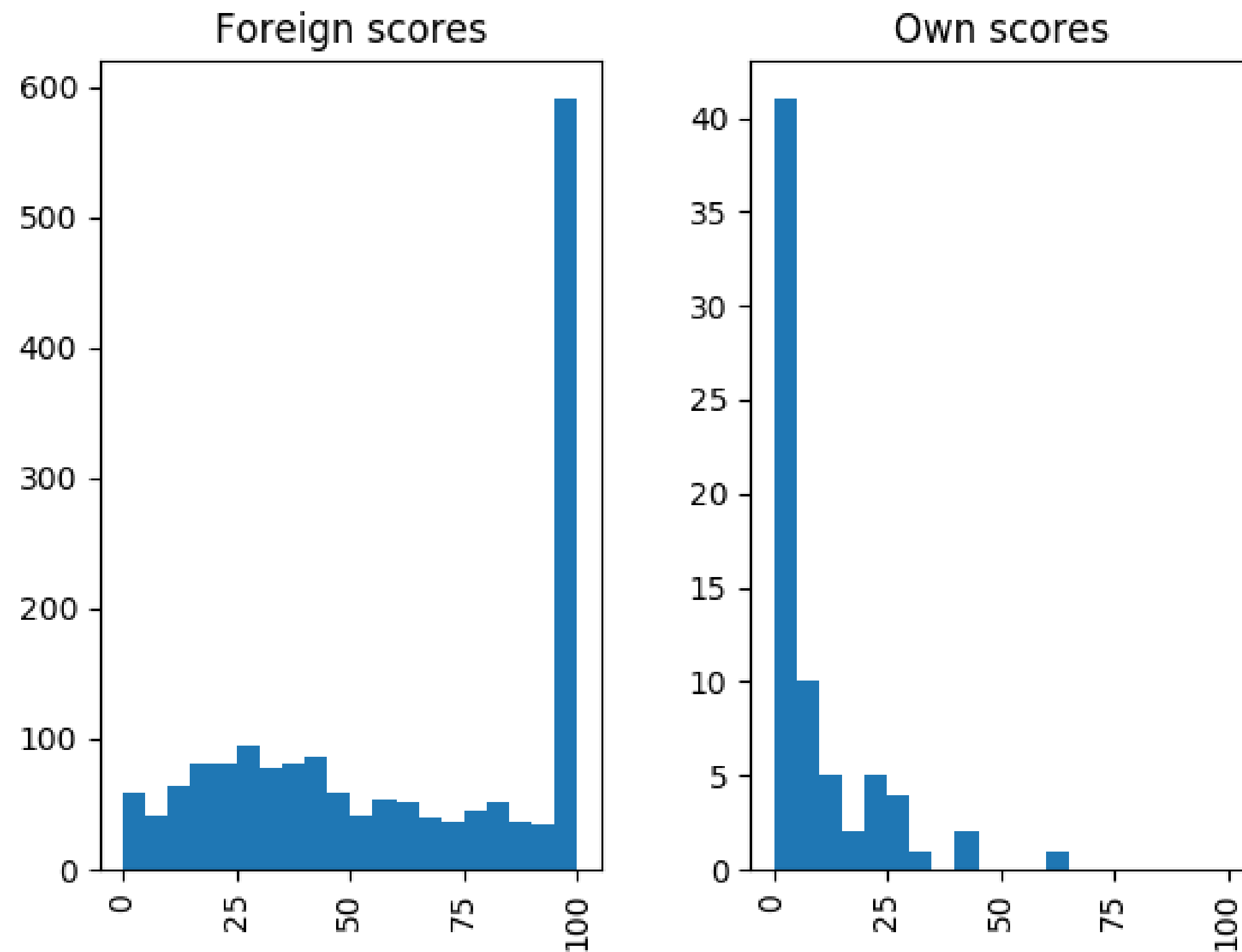
# Egér mozgás elemzés hatékonysága

**scbMouseUserAuth**

**AUC = 0.93**

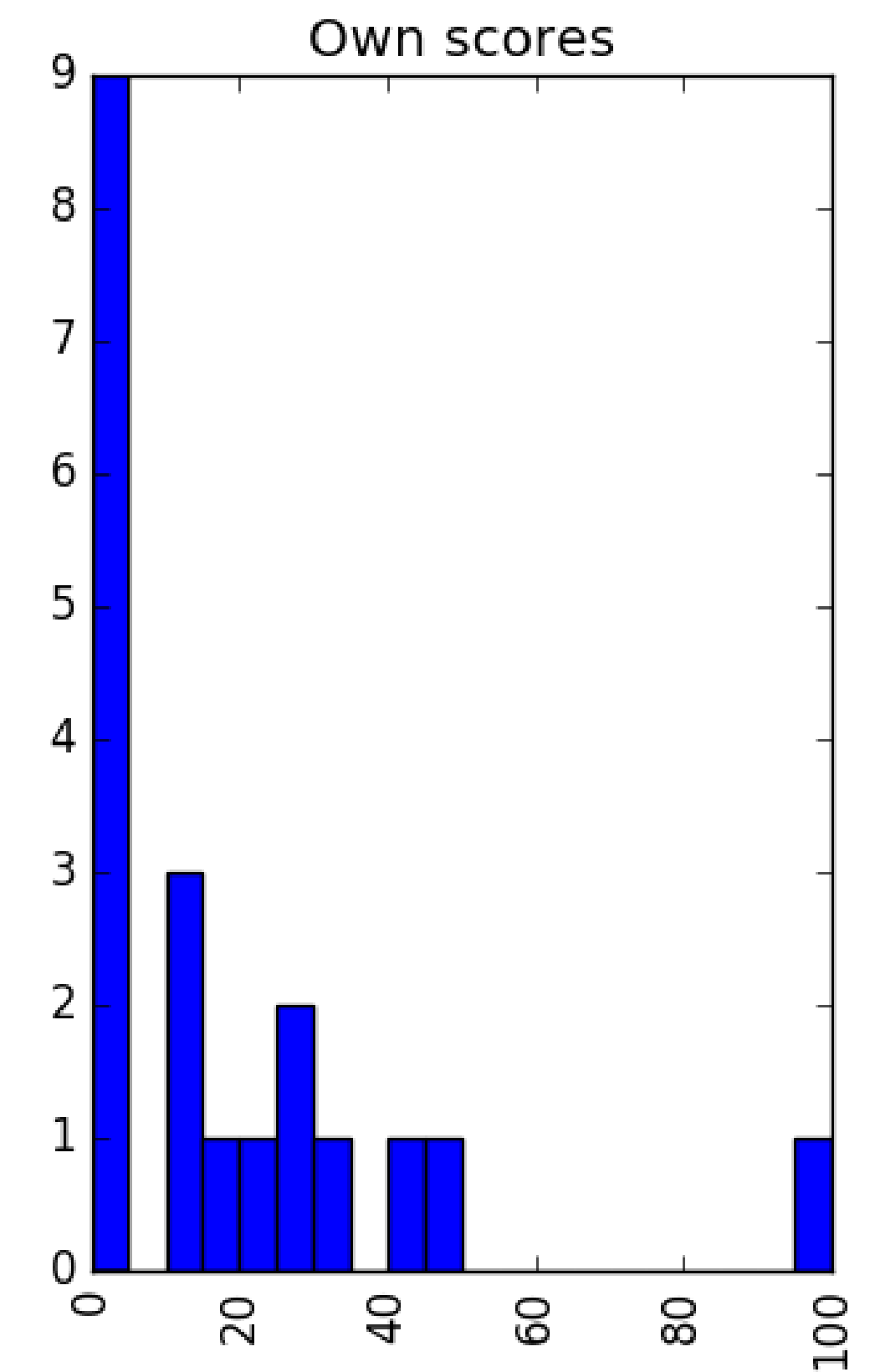
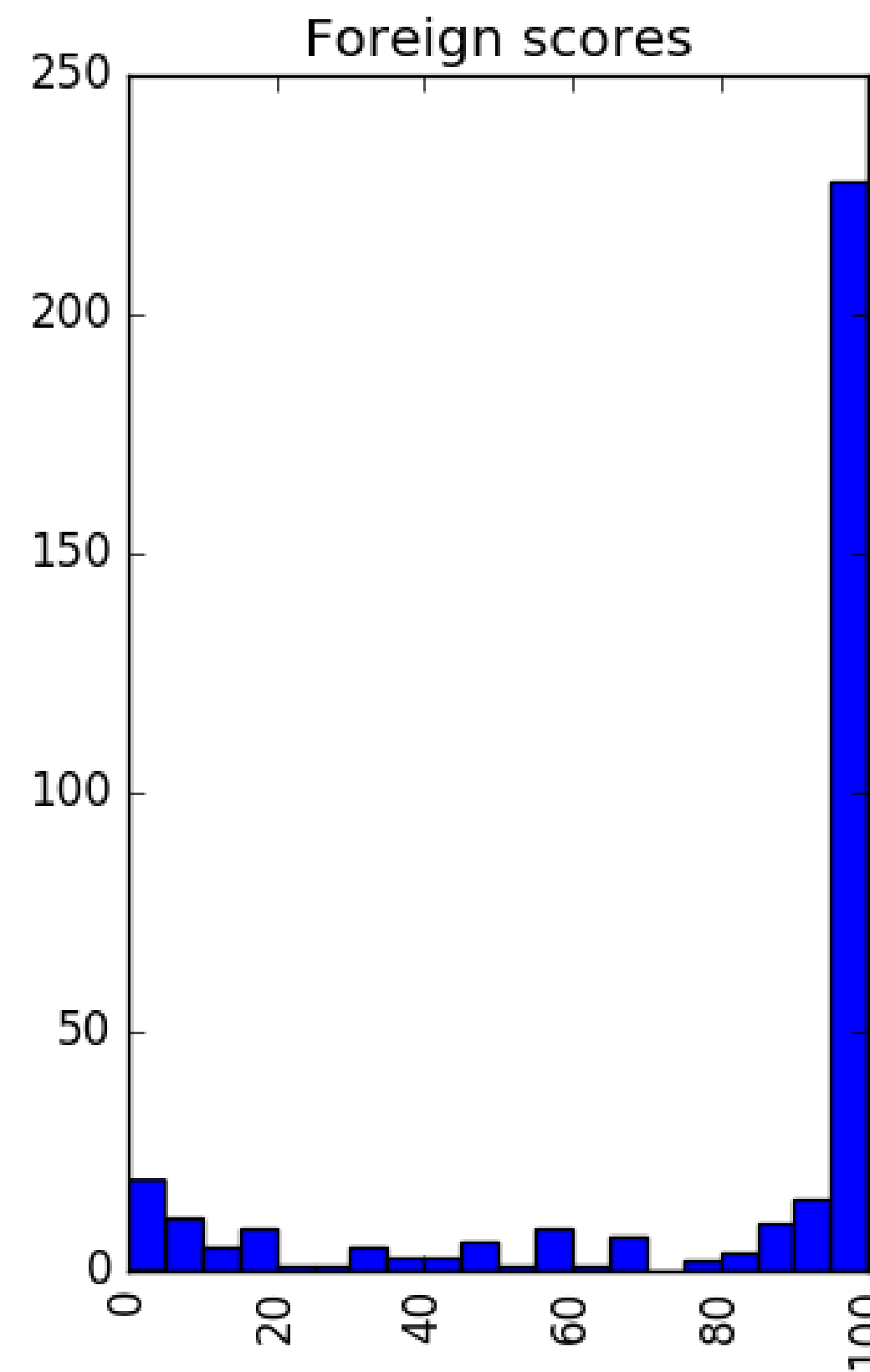
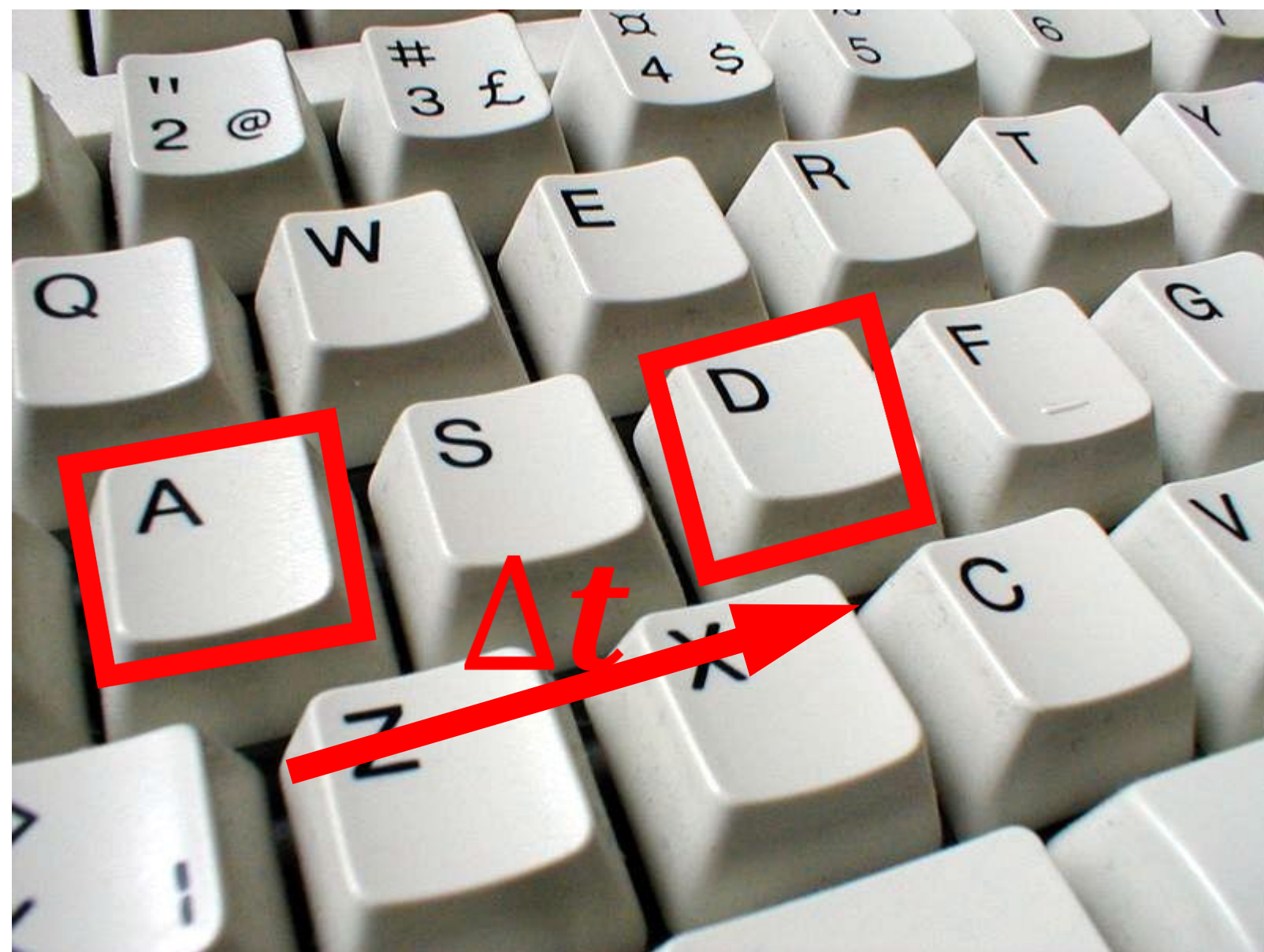
**Score distributions for scbMouseUserAuth**

**Receiver Operating Characteristic for scbMouseUserAuth**



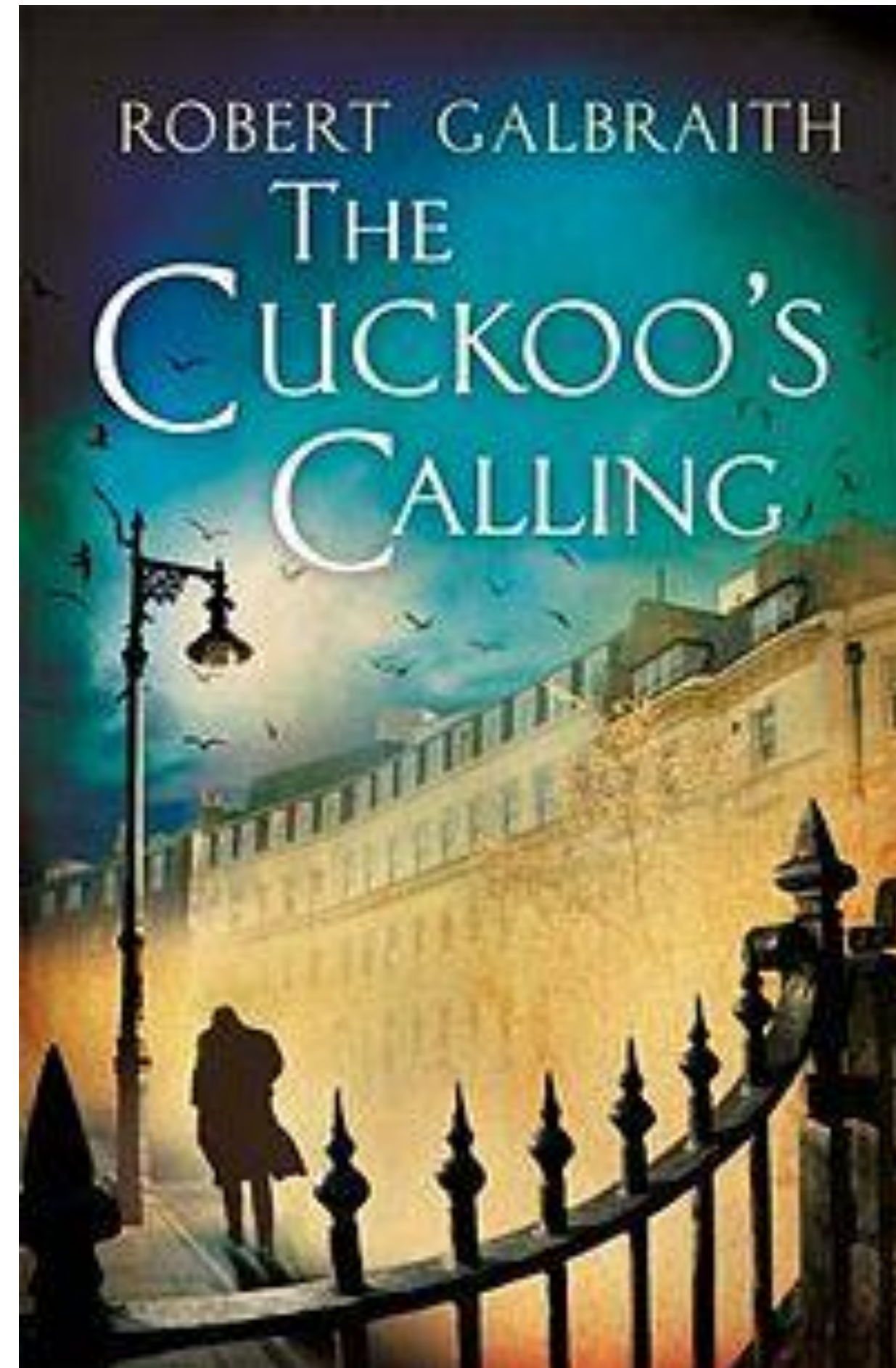
# Gépelési dinamika

AUC = 0.92



# TOVÁBBI ELEMZÉSI LEHETŐSÉGEK

# Írói stílus



# Ha nincs biometrikus adat...

- Command elemzés
- Window title
- Host login
- Login time
- Stb...

# Folyamatos autentikáció

- Felhasználók **digitális lábnyomának** begyűjtése
- Baseline építés a „**normális**” viselkedésre
- **Szokatlan** aktivitások valós idejű azonosítása
- Azonnali reakció, **az adatlopást megelőzésére**

