BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

PASSWORDS ARE DEAD! USER BEHAVIOR ANALYTICS

A sophisticated tool for detecting malicious insiders

Gabor Illes
Pre-sales engineer
gabor.illes@balabit.com

Tallin, Estonia
2016

EXISTING CONTROLS FOR PRIVILEGED USERS

PASSWORDS

MULTI-FACTOR AUTHENTICATION

PRIVILEGED IDENTITY / ACCESS MANAGEMENT

PRIVILEGED SESSION MONITORING

WHY DO WE NEED SOMETHING NEW?

TARGET

SOCIETE GENERALE

APTs, illegally acquired user credentials. Have you ever heard about...

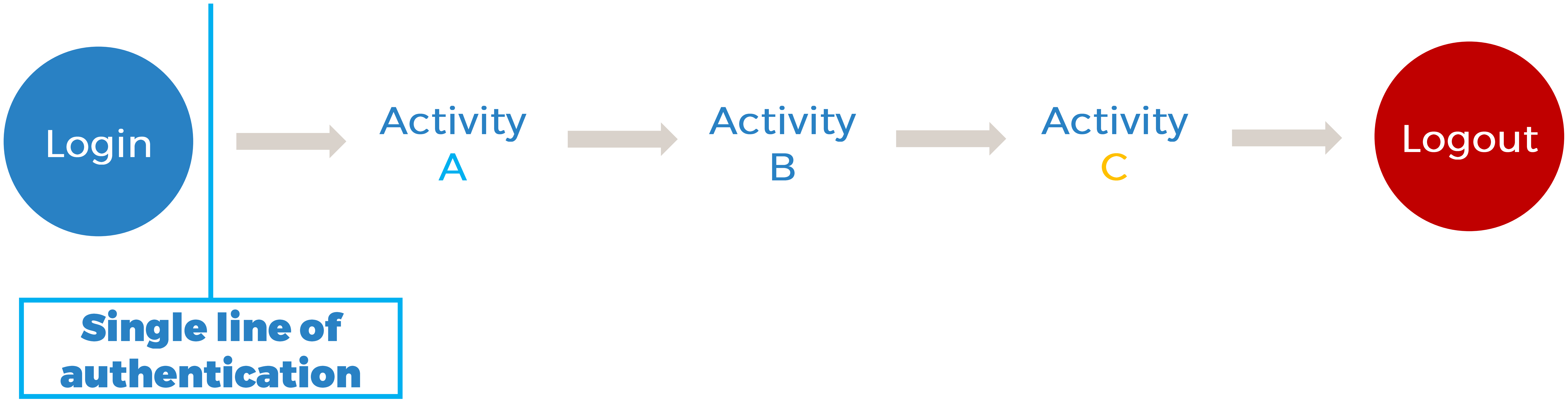
- Target?

Can you fully trust in your colleagues?

- Jérome Kerviel, Société Générale

WHAT IF THE ATTACKER ALREADY HAS ACCESS?

ONE-OFF AUTHENTICATION VS CONTINUOUS AUTHENTICATION



Login

Activity A

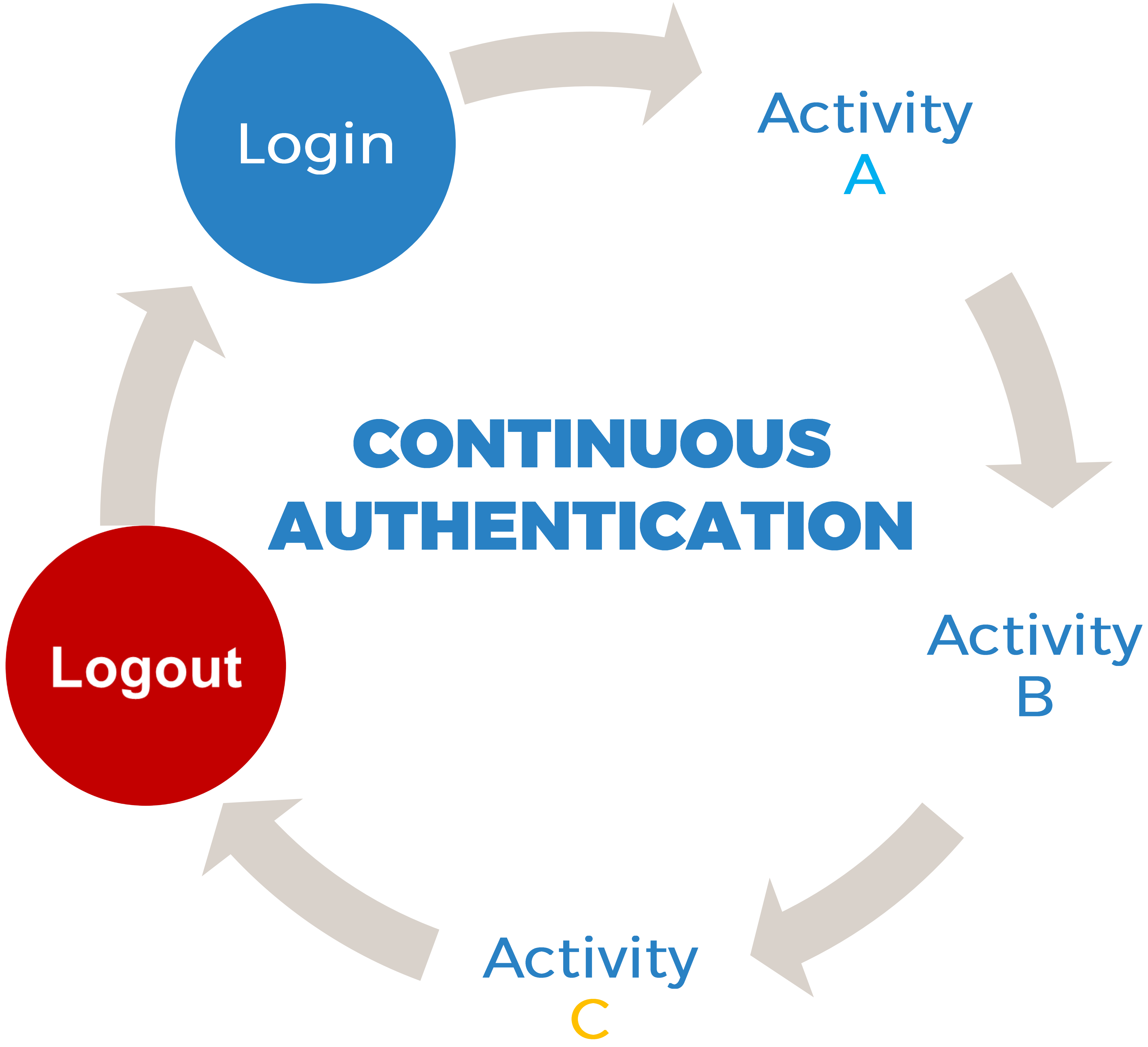
Activity B

Activity C

Logout

Single line of authentication

ONE-OFF AUTHENTICATION VS CONTINUOUS AUTHENTICATION



Login

Activity A

Activity B

Activity C

Logout

CONTINUOUS AUTHENTICATION

HOW CAN YOU IMPLEMENT CONTINUOUS AUTHENTICATION WITHOUT DRIVING YOUR EMPLOYEES MAD?

BALABIT

BEHAVIOR IS THE SOLUTION

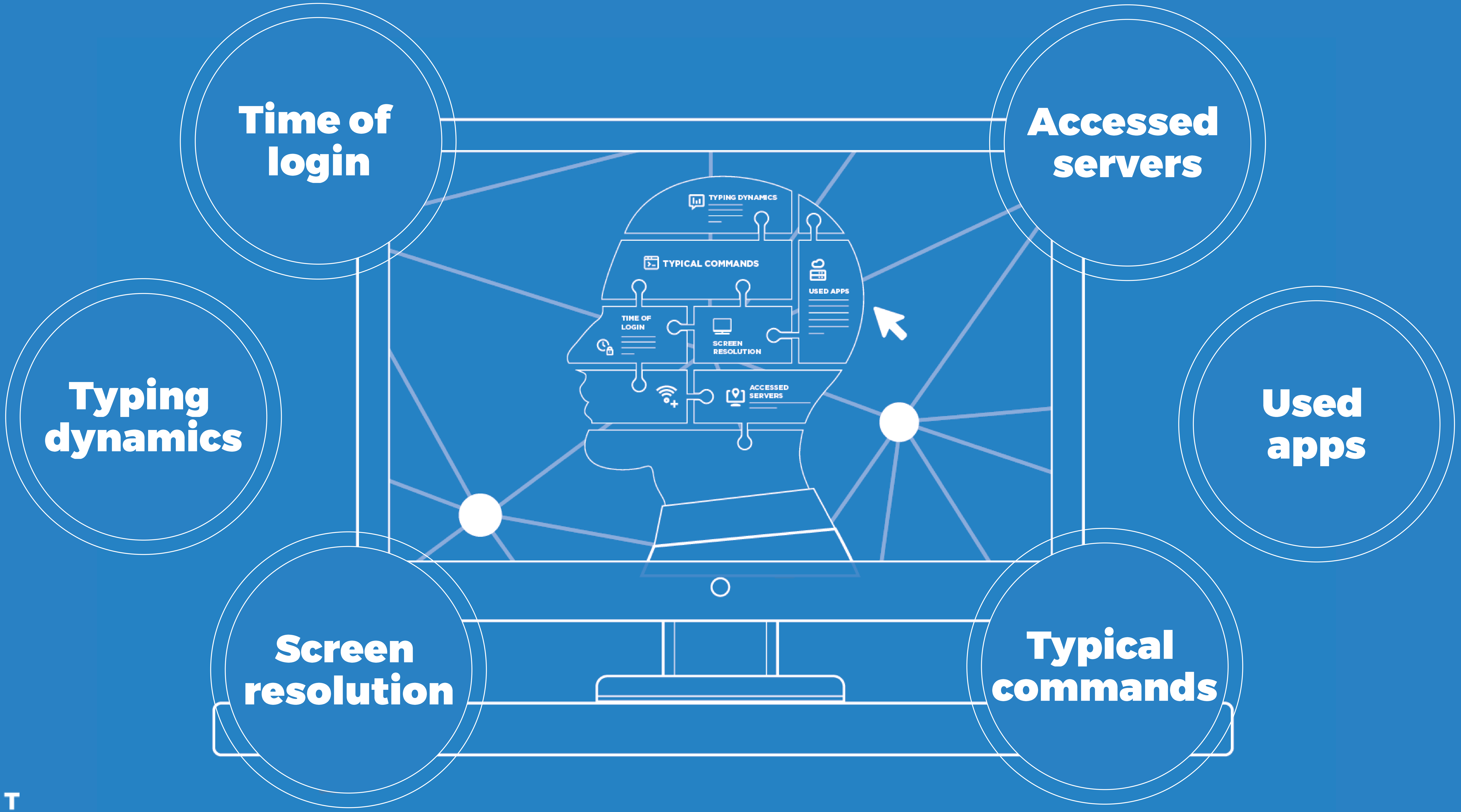
BALABIT

BEHAVIOR IS THE NEW AUTHENTICATION?

> “ **BEHAVIOR IS THE INTERNALLY COORDINATED RESPONSES OF WHOLE LIVING ORGANISMS TO INTERNAL AND/OR EXTERNAL STIMULI.** “

Daniel A. Levitis, PhD in Integrative Biology

WHAT IS DIGITAL BEHAVIOR?



Time of login

Accessed servers

Typing dynamics

Used apps

Screen resolution

Typical commands

HOW CAN BEHAVIOR ANALYSIS PREVENT ATTACKS?

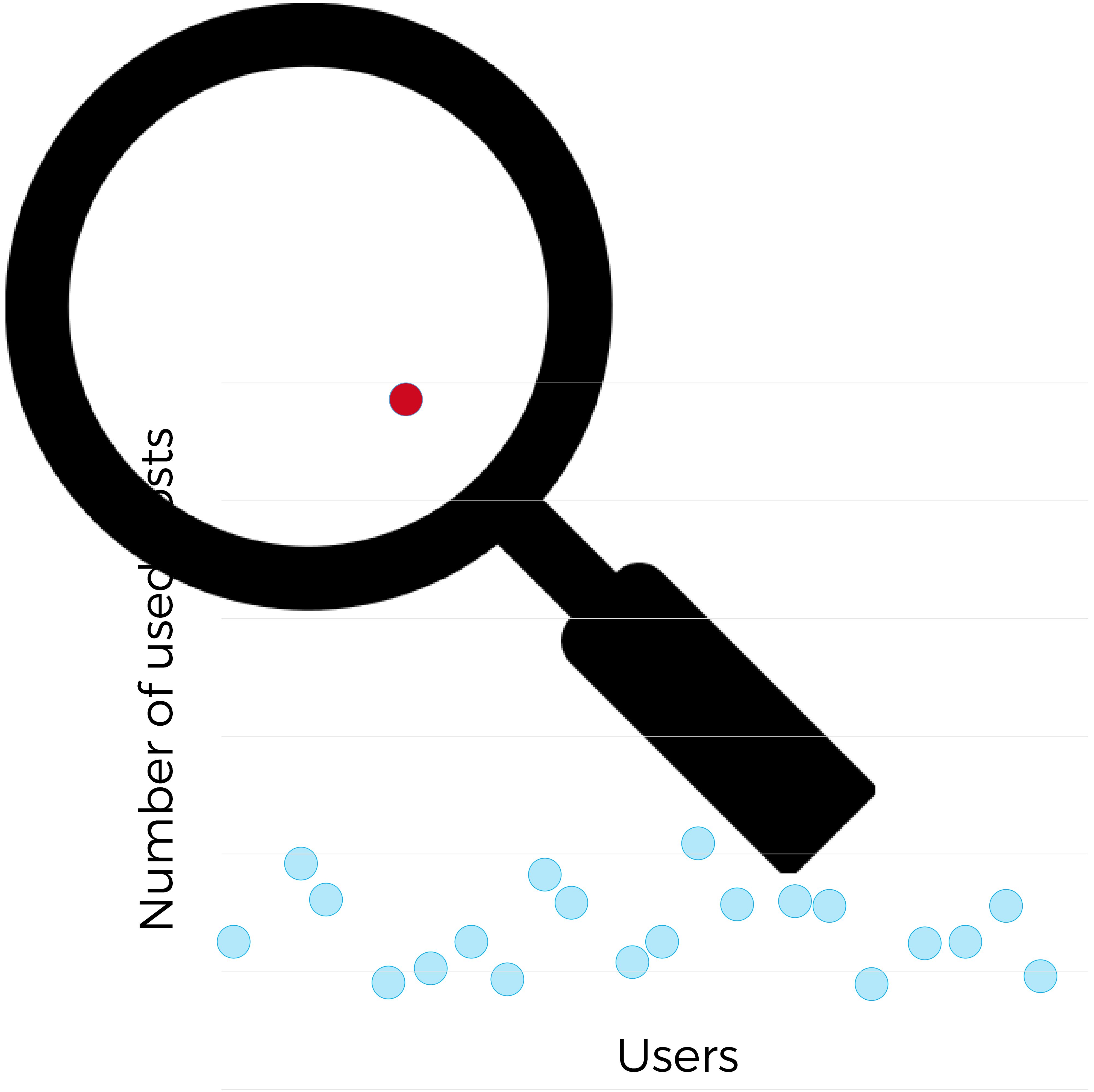
GATHER users' **DIGITAL FOOTPRINTS**

DEFINE what is **NORMAL**, build user baselines

Identify UNUSUAL EVENTS in real-time

Identify EXTERNAL attackers

Identify malicious INSIDERS



BEHAVIOR IS THE NEW AUTHENTICATION!

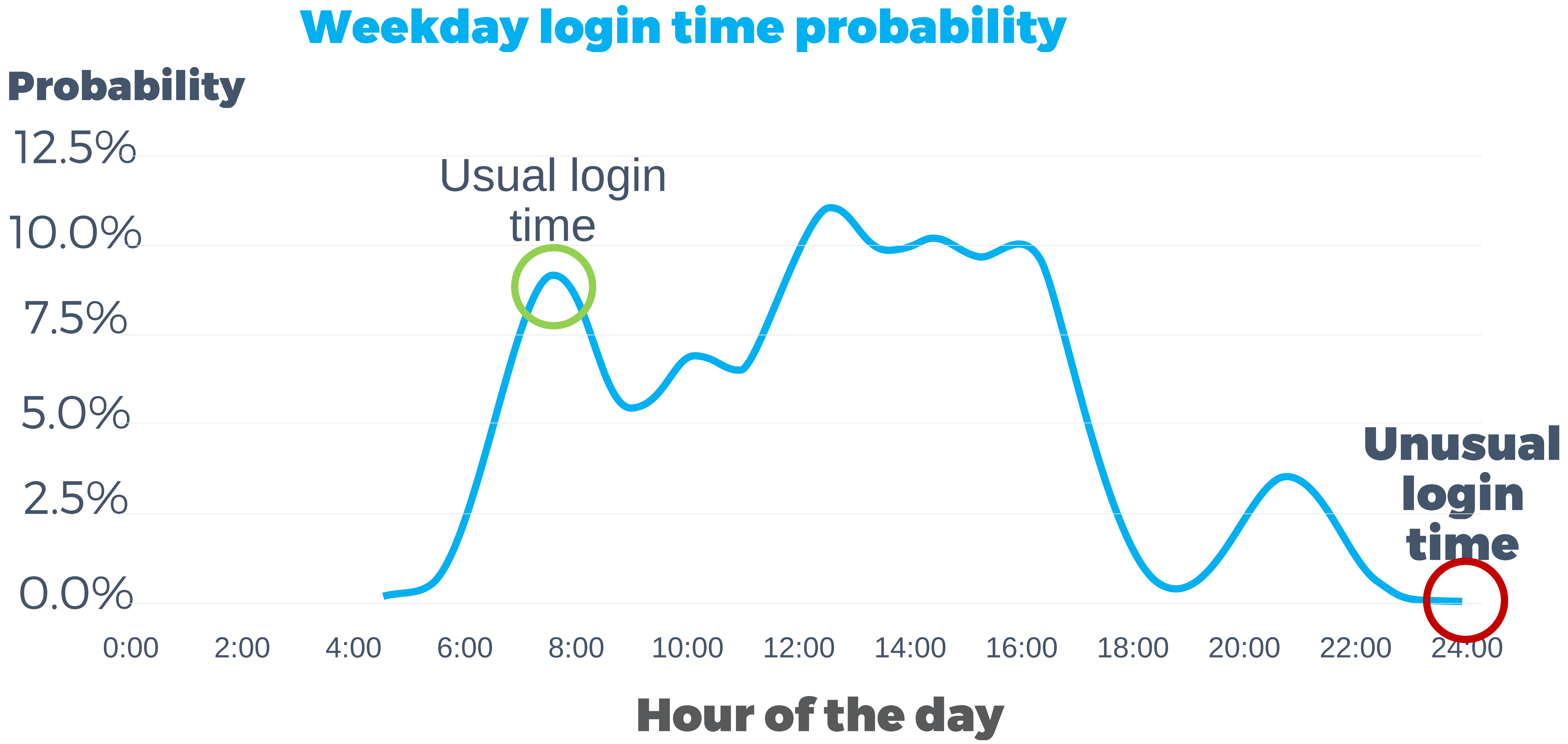
HABITS

Something you do

Typical time of working

Typical activities performed (Commands in CLI, Applications in GUIs, Transaction types)

Range of accessed servers and applications



BEHAVIOR IS THE NEW AUTHENTICATION!

POSSESSION

Something
you have

Screen resolution

Mouse vs trackpad vs touchscreen

Type and version of the operating system, browser & client apps

Browser settings (Language, Time zone)

BEHAVIOR IS THE NEW AUTHENTICATION!

INHERENCE

Something you are

Mouse movement analysis

Keystroke dynamics analysis

BEHAVIOR IS THE NEW AUTHENTICATION!

CONTEXT

Something that surrounds you

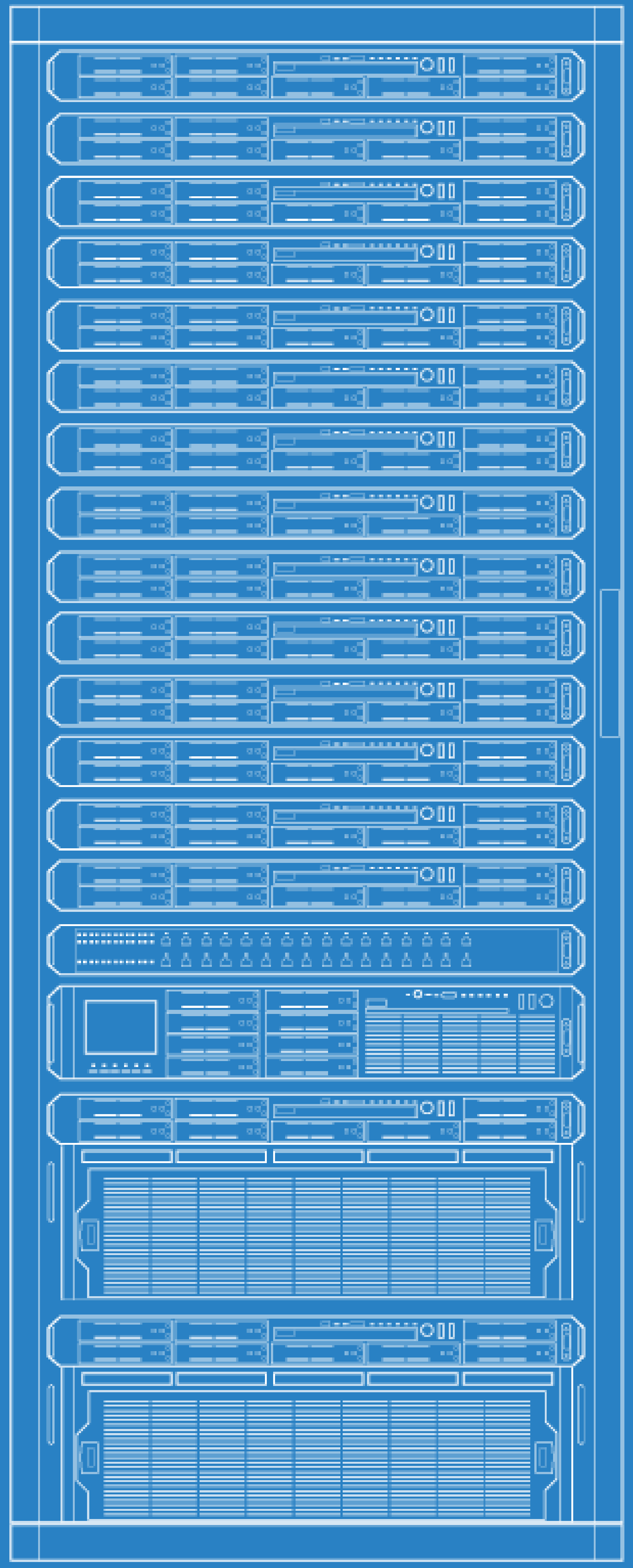
Location (GeoIP, ISP, GPS data)

Network traffic counters

IP address reputation

PASSWORDS ARE DEAD ?

Authentication does not defend against those attackers, who have valid credentials (malicious insiders, APT attacks)



Advantages of user behavior analytics:

- Continuous
- Detect changes and anomalies
- Biometrics is very hard to imitate

THREE KEY ISSUES FOR SECURITY PROS

COST OF COMPLIANCE

Where should we prioritise spend?

How can we leverage our existing investments?

PREVENTING DATA BREACHES

Can we react fast enough to an insider threat or APT attack?

SOC EFFICIENCY

Too much data, too many false positives, too few analysts

Q&A

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

THANK YOU FOR YOUR ATTENTION!

More information: www.balabit.com

2016