Contextual Security Intelligence

Preventing Data Breaches without Constraining Business

Beograd 2016

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

200+ employees

> 50% y/y growth over year

100+ resellers

London
Tower 42, 25 Old Broad Street, London EC2N 1HN

Paris
105, rue Jules Guesde, 92300 Levallois Perret

Munich
Stefan-George-Ring 29. D-81929 München

Budapest
Alíz street 2. H-1117 Budapest

New York
40 Wall St. 28th Floor, NYC, NY 10005

1300+ Customers

BALABIT

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Founded: **2000**

Customers: **1300+**

Users: **1M+**

Specializing: **log management, advanced monitoring, user behavior analytics**

TRADITIONAL APPROACHES ARE NOT ENOUGH...

BALABIT

TRADITIONAL APPROACHES ARE NOT ENOUGH...

Impossible to pre-define all rules

BALABIT

TRADITIONAL APPROACHES ARE NOT ENOUGH...

- Impossible to pre-define all rules
- Constant fear of breaches

BALABIT

TRADITIONAL APPROACHES ARE NOT ENOUGH...

- Impossible to pre-define all rules
- Constant fear of breaches
- Activities without context

BALABIT

HUMANS ARE THE NEW PERIMETER

”Professionals are target people. And any solutions will have to target the people problem, not the math problem”

"...nearly 90% of all incidents – is people."

CONTEXTUAL SECURITY INTELLIGENCE

Immediate reaction

Real-time knowledge of all actions

Recognition of the unusual

Norm and pattern recognition and learning

BALABIT

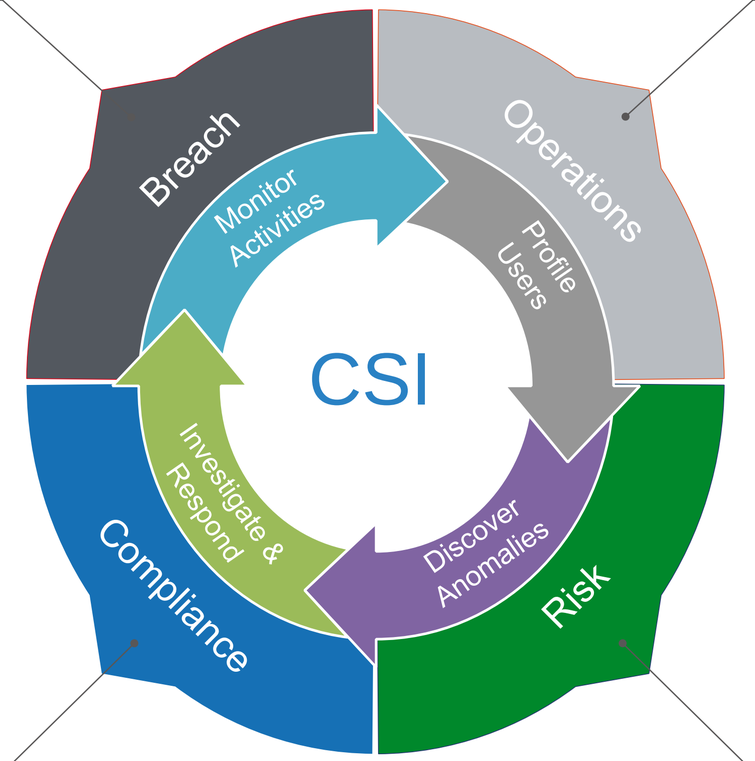
Benefits areas

Breach Prevention

Intervention at the most relevant step of the kill chain

Security Operations

Real-time behavior intelligence
Efficient forensic investigations



Compliance ROI

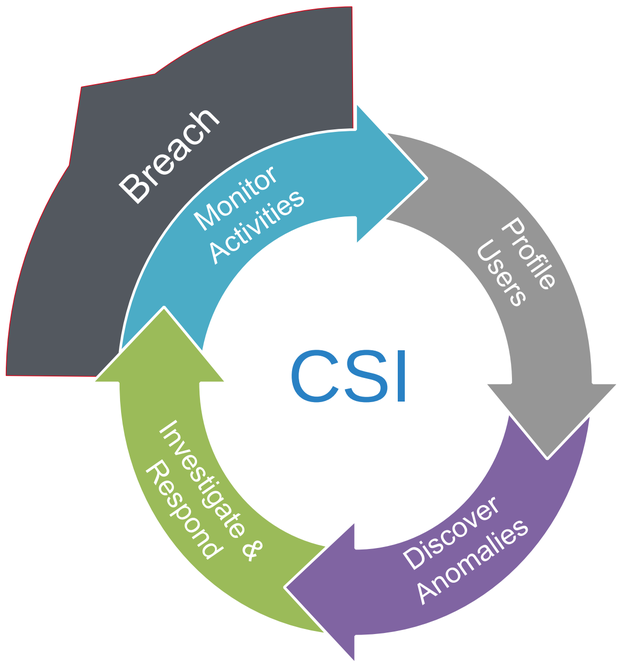
Comprehensive overview of privileged activities
Decreased cost of compliance

Risk Assessment

Policy breach & account risk detection

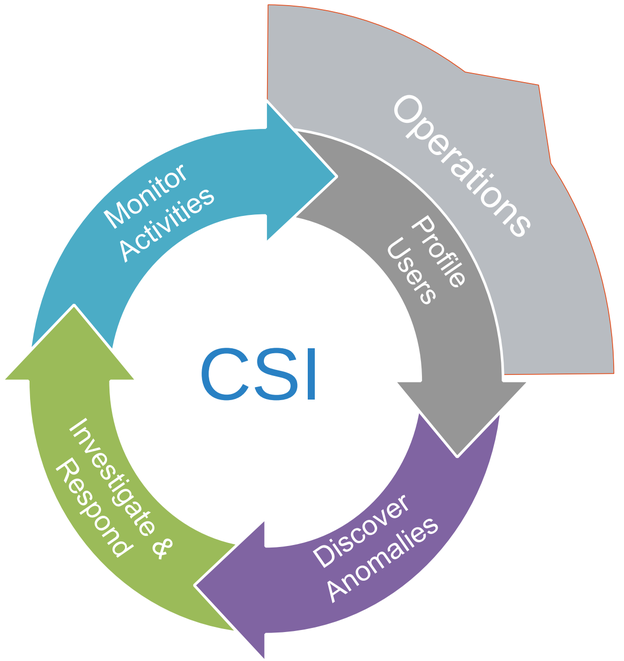
Breach Prevention

- Identify malicious activity by detecting unusual behavior patterns
  - Date, time, geo, commands, keystrokes, mouse, peer group outliers, etc.
- Insider threats and hijacked accounts
- APT Kill Chain
  - Intervention at the most relevant step of the kill chain



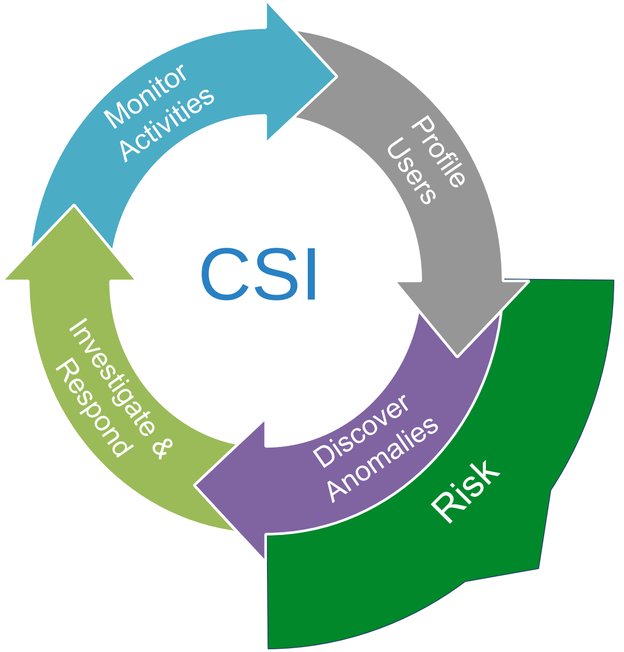
Security Operations

- Efficient incident response & forensics capabilities
- Real time behavior intelligence through alerts
- Automated security reactions & intervention



Risk Assessment

- Account and global risk estimation
- Identifying account related policy violations
- Identify the gap between the privileges and actual behavior

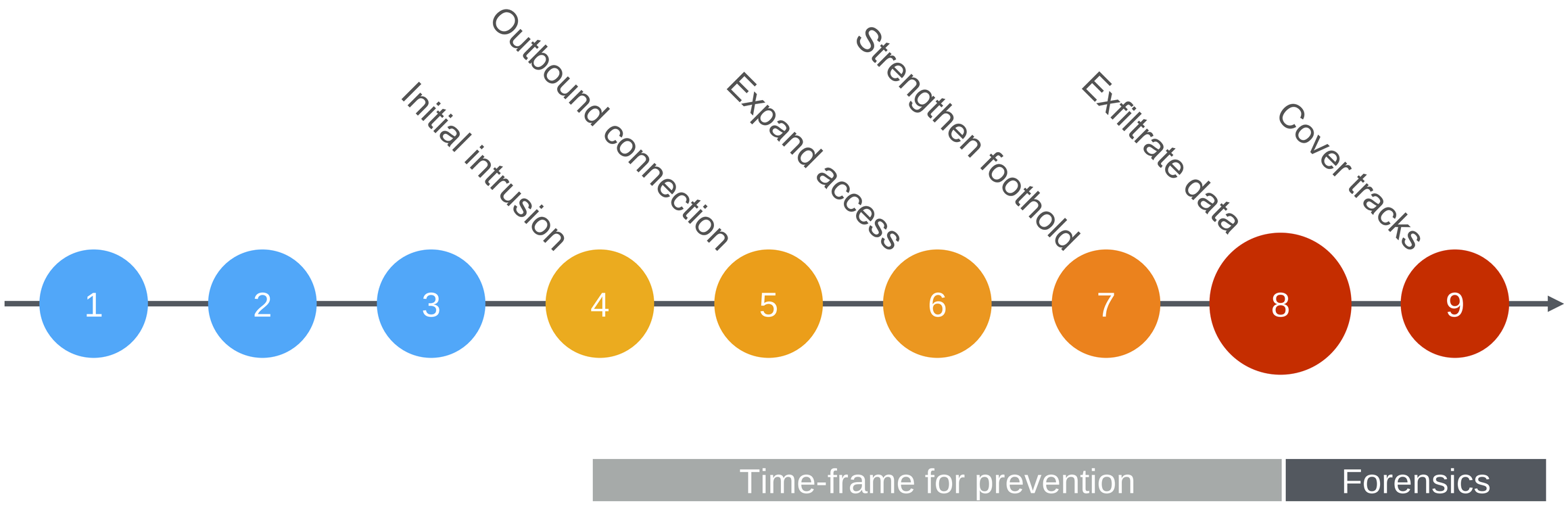


Compliance ROI

- Comprehensive audit and review of application and system level access
- Compliance Plus – integrating existing data recorded for compliance reasons into CSI to unveil security risks
- Prioritize recorded audit trails based on risk

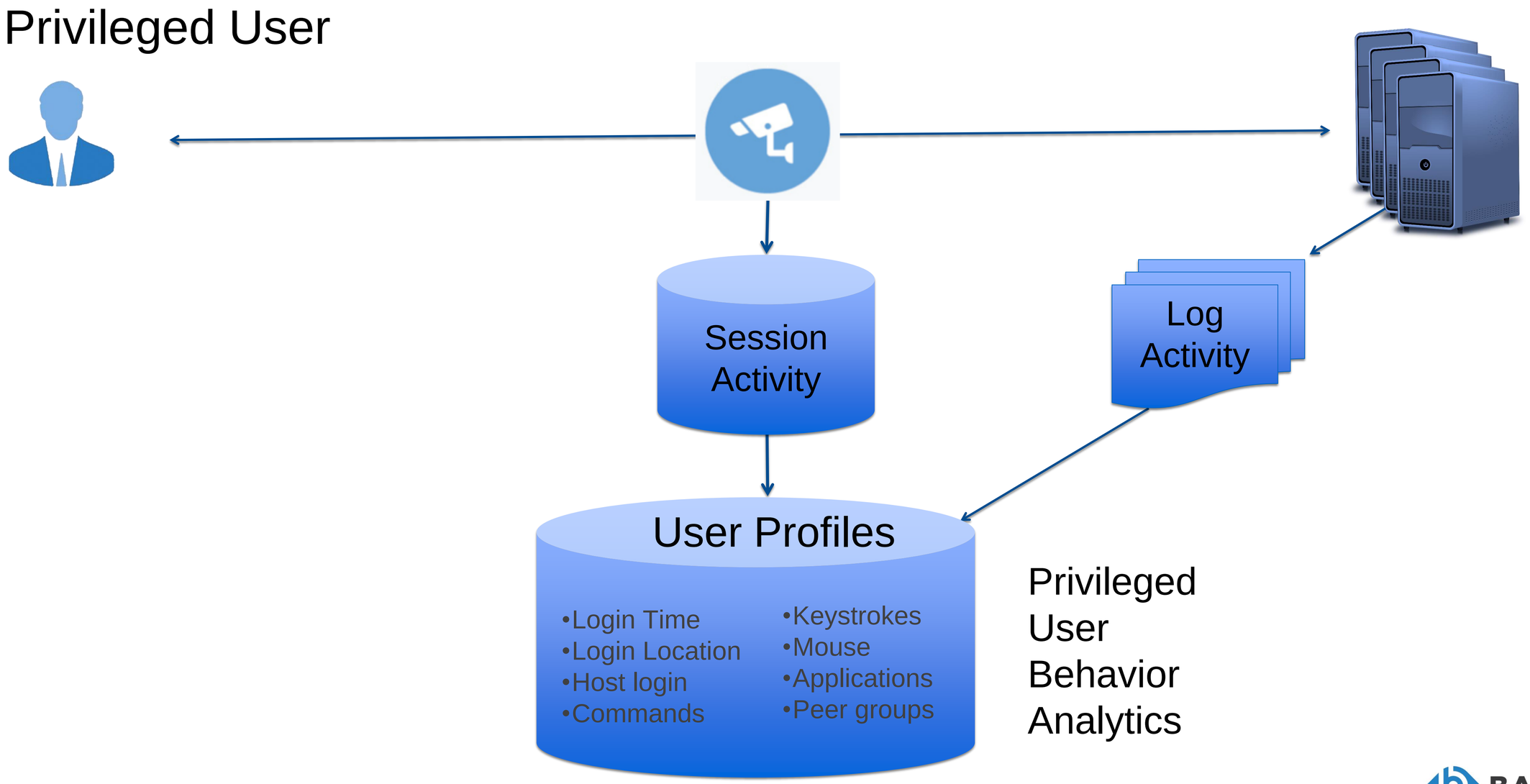
PREVENTION BY MONITORING

LET'S EXAMINE A HUMAN ATTACK!



BALABIT

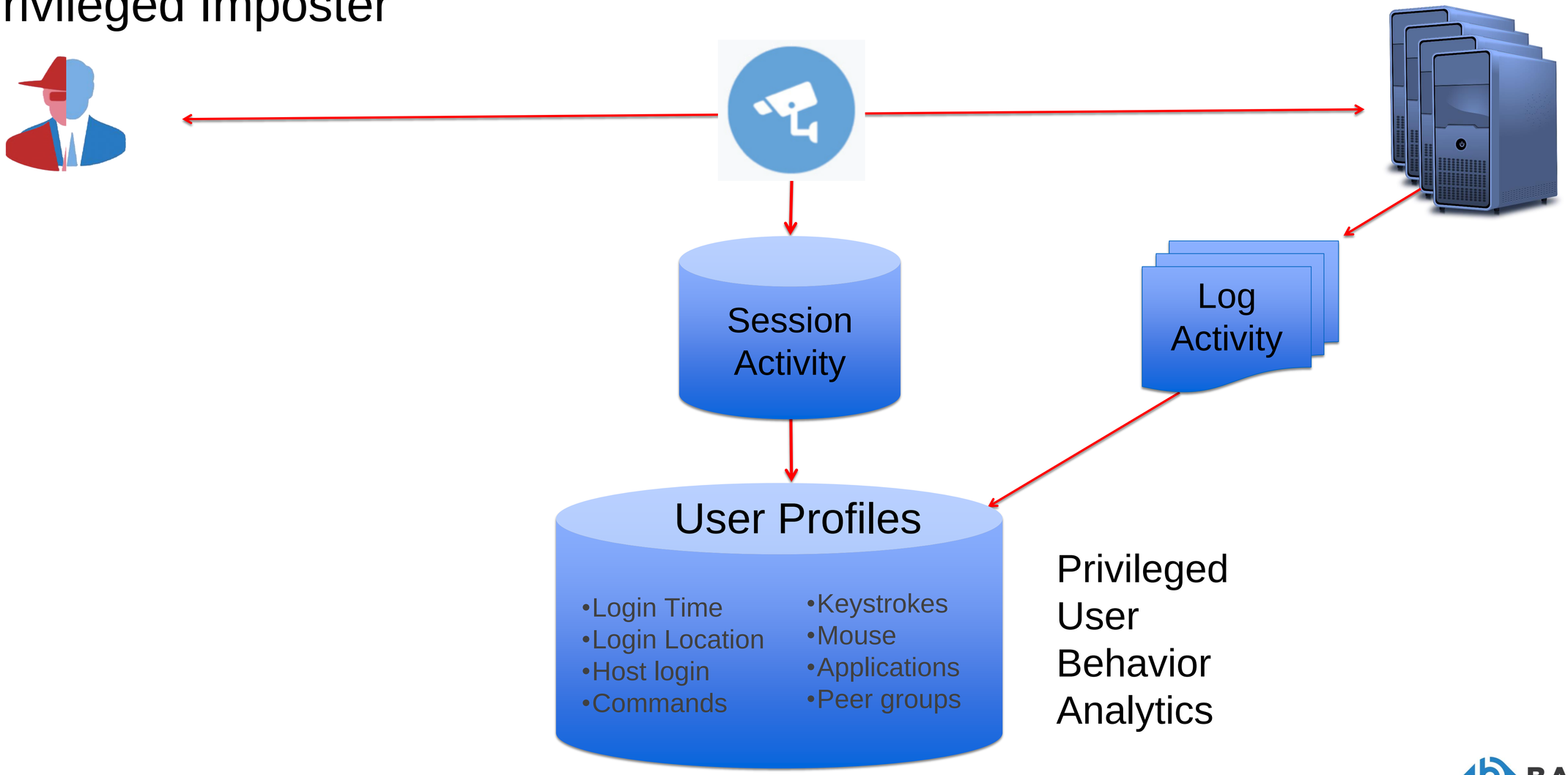
CONTEXTUAL SECURITY INTELLIGENCE SUITE IN ACTION



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE SUITE IN ACTION

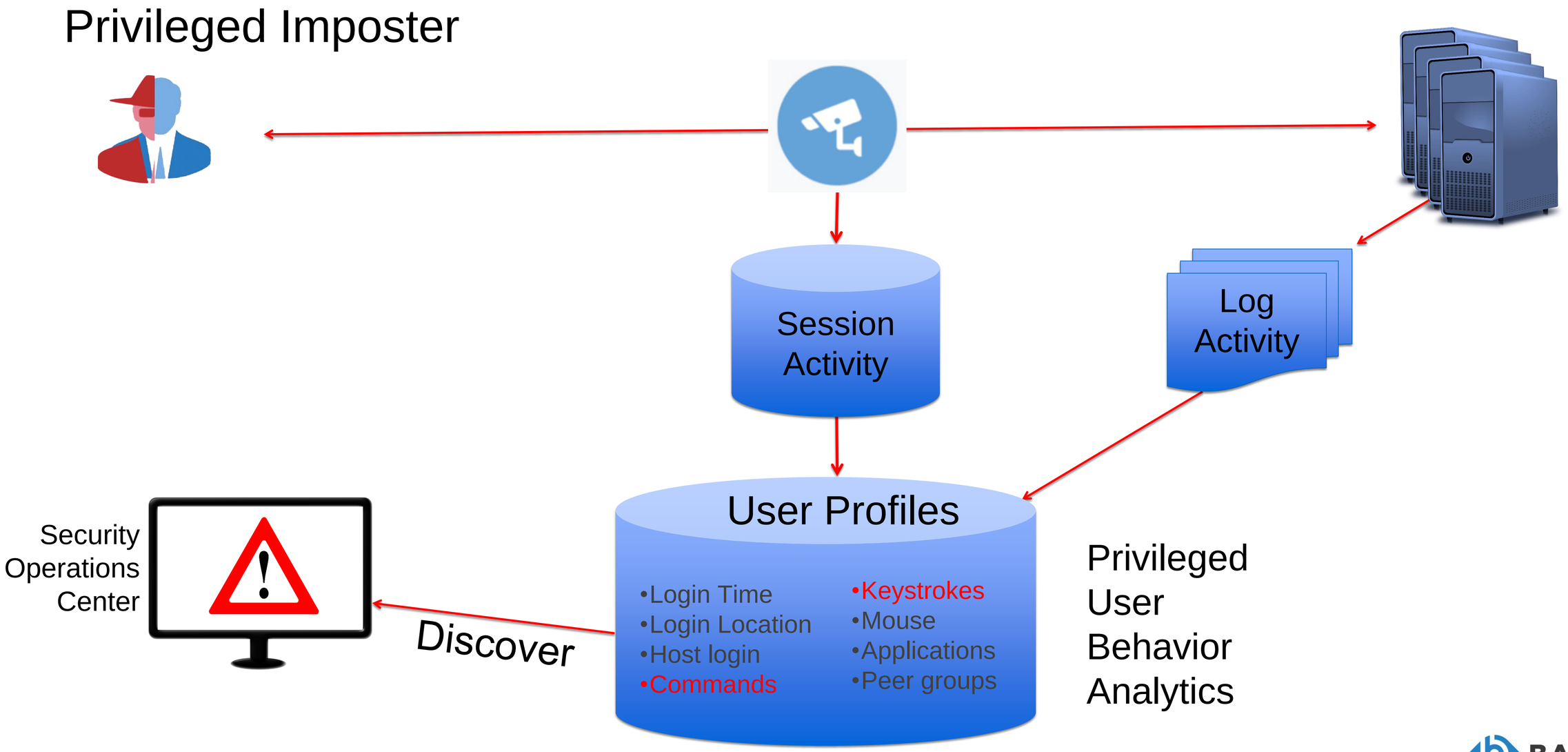
Privileged Imposter



Privileged User Behavior Analytics

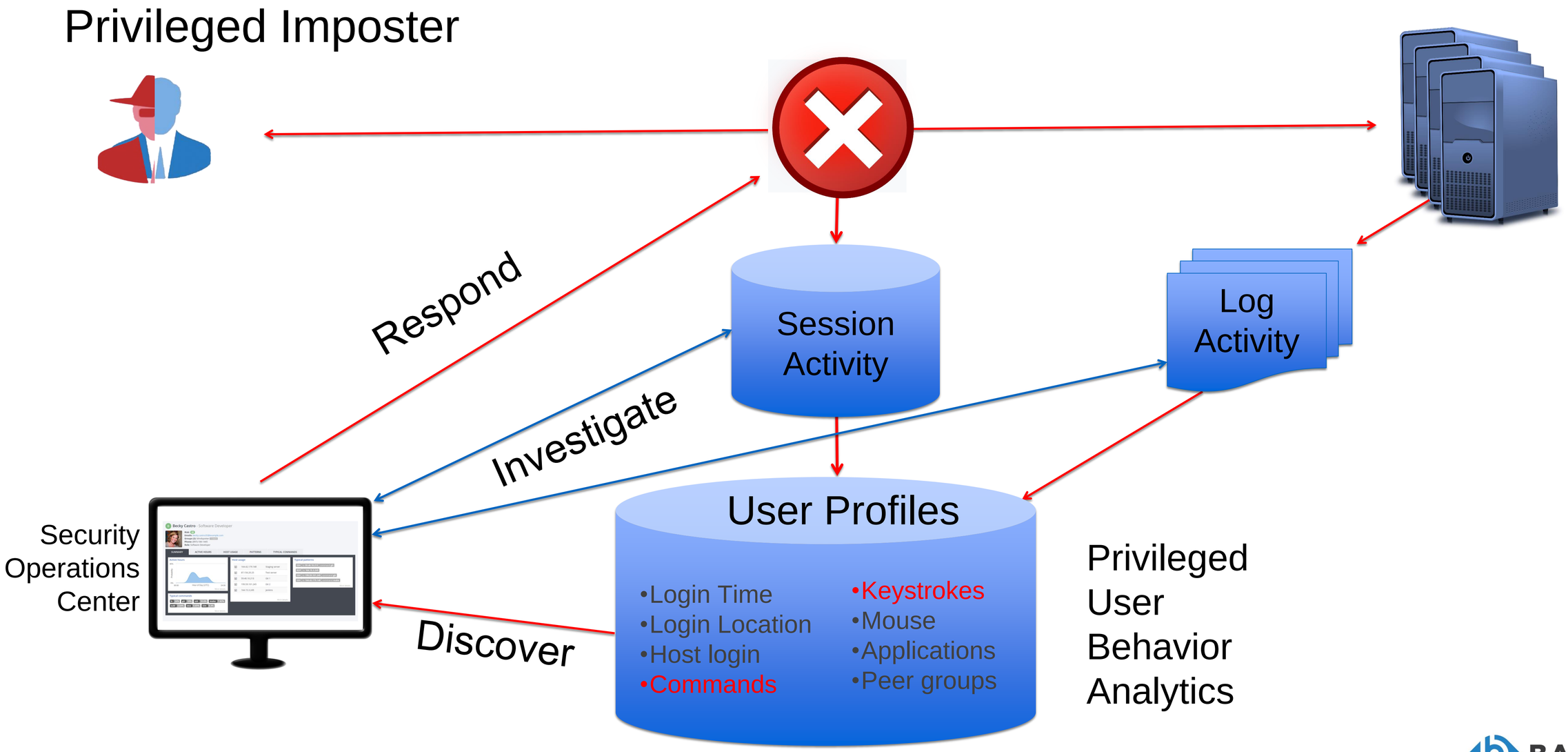
BALABIT

CONTEXTUAL SECURITY INTELLIGENCE SUITE IN ACTION



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE SUITE IN ACTION



BALABIT

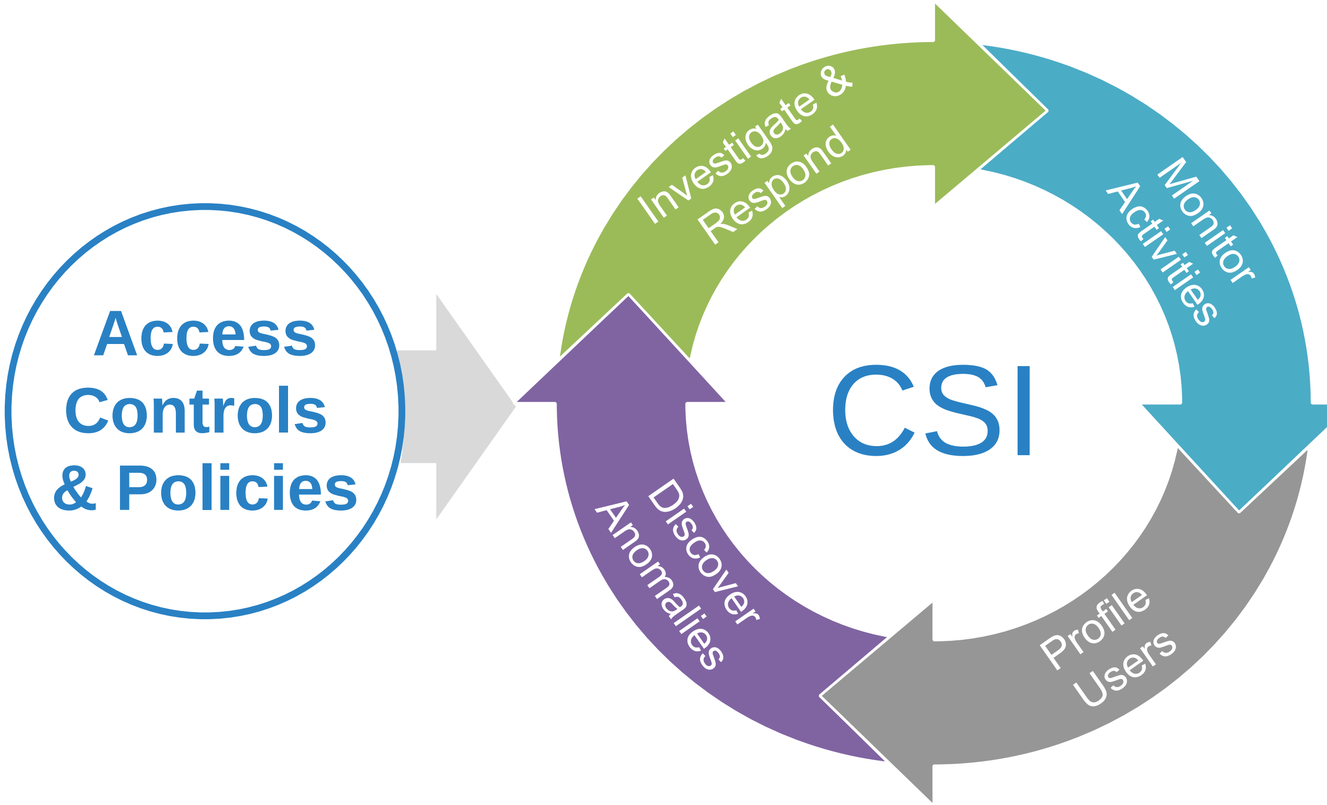
BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

CSI JOURNEY

Move from preventive to contextual security

- Monitor user activity
- Baseline business-as-usual using machine learning
- Discover unknown threats based on deviation from the norm and risk in real-time
- Investigate and respond immediately



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE LAYERS

The Problem

Vast amount of data	Understanding the situation	Not asked and not known

The Solution

CSI.DATA

Enriched Data Platform

- Instant access to activity data in forensic situations.
- Activity & log data collection across the entire enterprise
- Transparent session monitoring with agentless deployment
- Real-time data delivery for analytics and investigation
- Filtering, normalization and enrichment

CSI.USER

The User Perspective

- Integrate contextual information into a single profile
- Drill down into CSI.DATA for deeper understanding
- Video replay & search in user recordings
- Visualize normal behaviour

CSI.RISK

Behavioural Analytics

- Machine learning of activities
- Anomaly Detection
- Real-time intervention
- Risk scoring and alerting

BALABIT

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

CSI.DATA: GATHERING THE FOOTPRINTS

ANY ANALYTICS IS ONLY AS GOOD AS THE DATA THAT FEEDS IT!

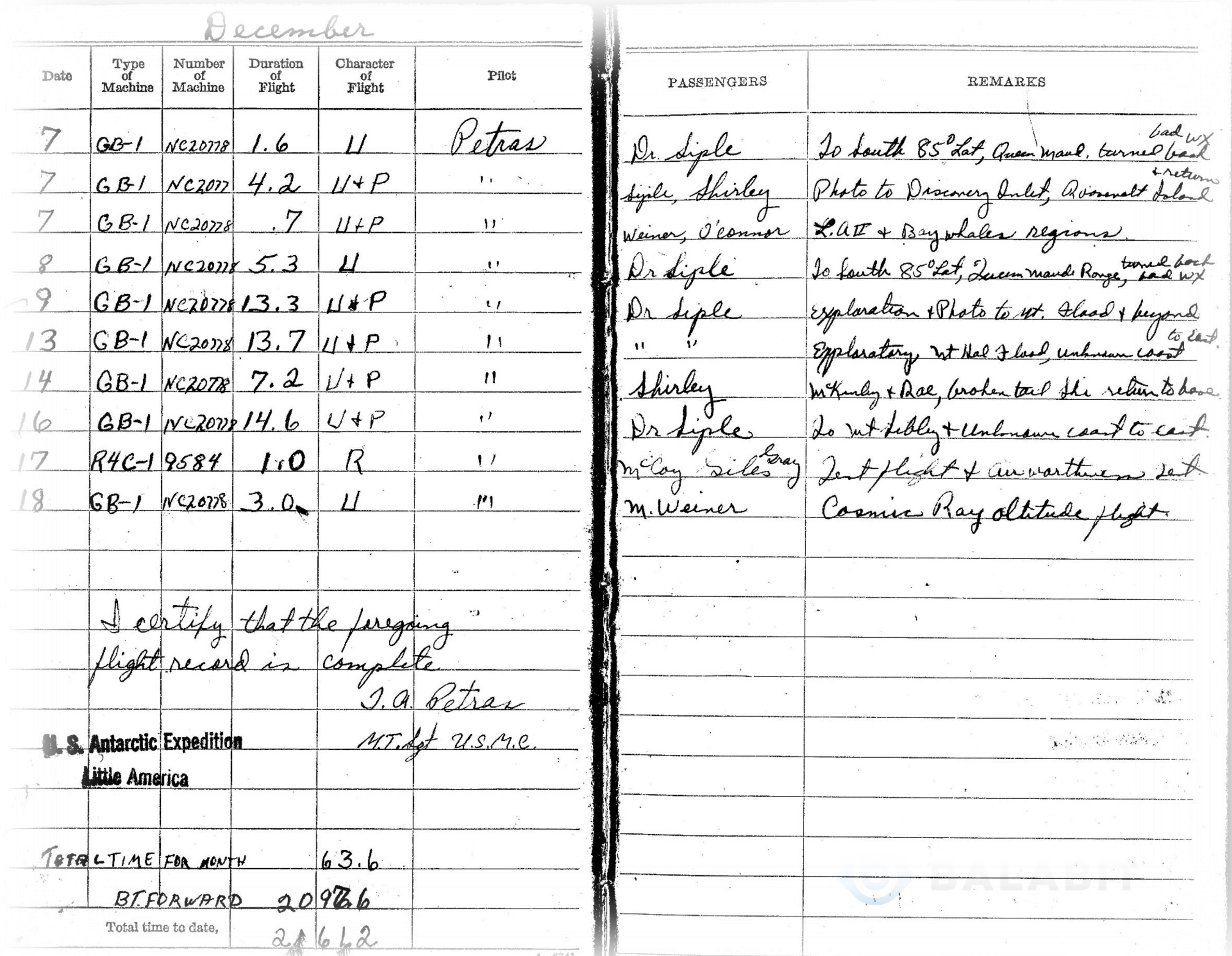
BALABIT

Syslog-NG & Syslog-ng STORE BOX

BALABIT

HIGH VOLUME, HIGH SPEED DATA: LOGS - SYSLOG-NG

- Information on all activities from the systems
- Reliable and secure collection, transport and storage
- Advanced processing & filtering



December

Date	Type of Machine	Number of Machine	Duration of Flight	Character of Flight	Pilot	Passengers	Remarks
7	GB-1	NC20778	1.6	U	Petras	Dr. Siple	To South 85° Lat, Queen Maud, turned back bad wx
7	GB-1	NC2077	4.2	U+P	"	Siple, Shirley	Photo to Discovery Inlet, Roosevelt Island + return
7	GB-1	NC20778	.7	U+P	"	Weiner, O'Connor	L.A II + Bay whales regions
8	GB-1	NC20778	5.3	U	"	Dr Siple	To South 85° Lat, Queen Maud Range, turned back bad wx
9	GB-1	NC20778	13.3	U+P	"	Dr Siple	Exploration + Photo to Mt. Hal Flood + beyond
13	GB-1	NC20778	13.7	U+P	"	" "	Exploratory, Mt Hal Flood, unknown coast to east
14	GB-1	NC20778	7.2	U+P	"	Shirley	McKinley + Rae, broken tail ski return to base
16	GB-1	NC20778	14.6	U+P	"	Dr Siple	To Mt Sidley + Unknown coast to east
17	R4C-1	9584	1.0	R	"	McCoy Giles Gray	Test flight + airworthiness test
18	GB-1	NC20778	3.0	U	"	M. Weiner	Cosmic Ray altitude flight

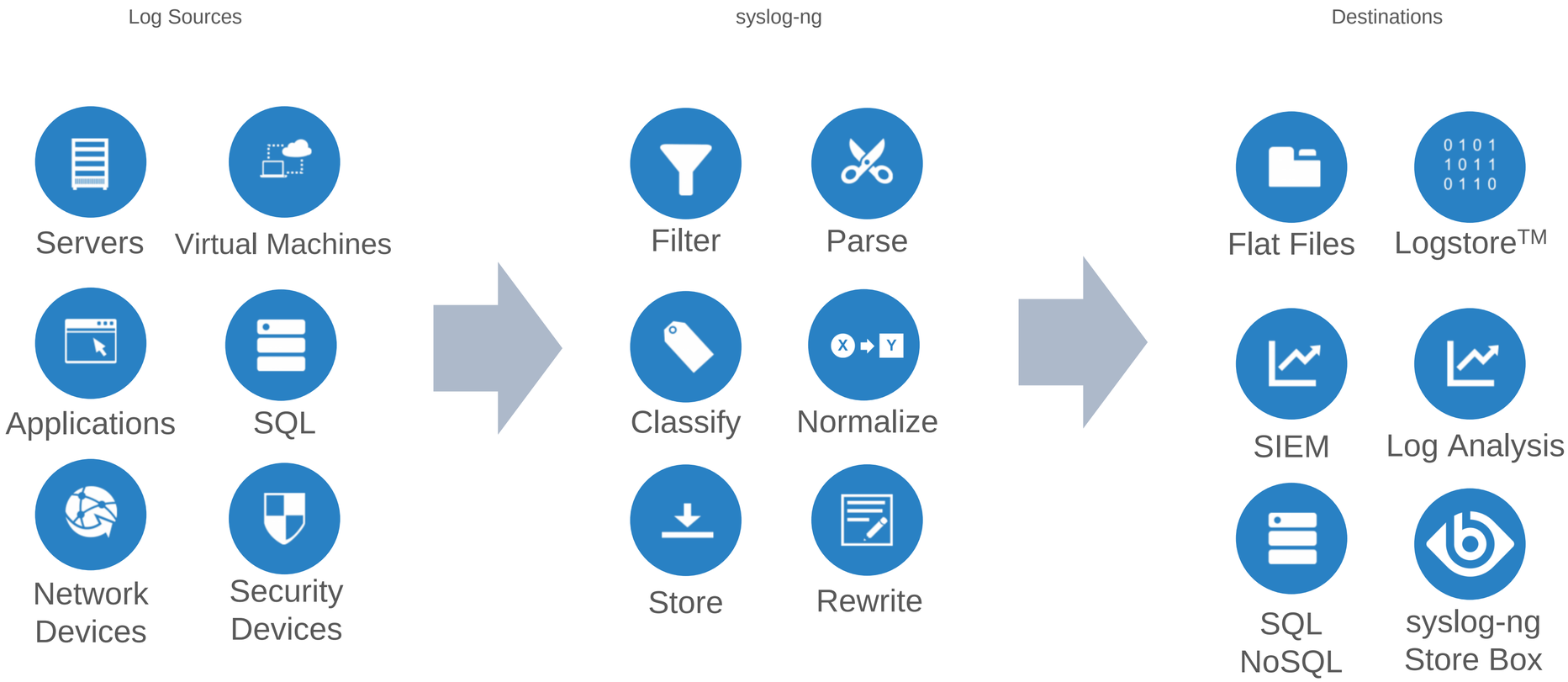
I certify that the foregoing flight record is complete.
T. A. Petras
M.T.Sgt U.S.M.C.

U. S. Antarctic Expedition
Little America

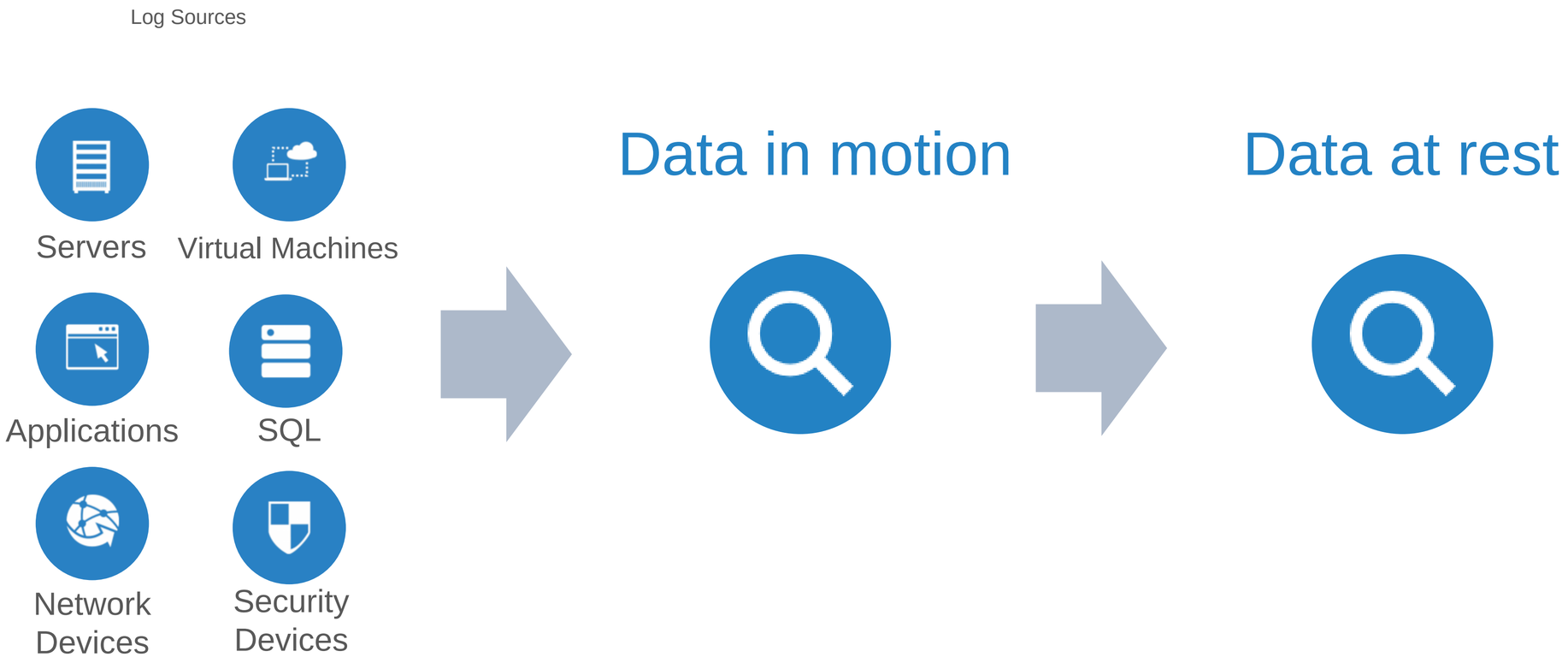
Total time for month 63.6
Bt. forward 209[illegible]6
Total time to date, 2[illegible]6[illegible]2

BALABIT

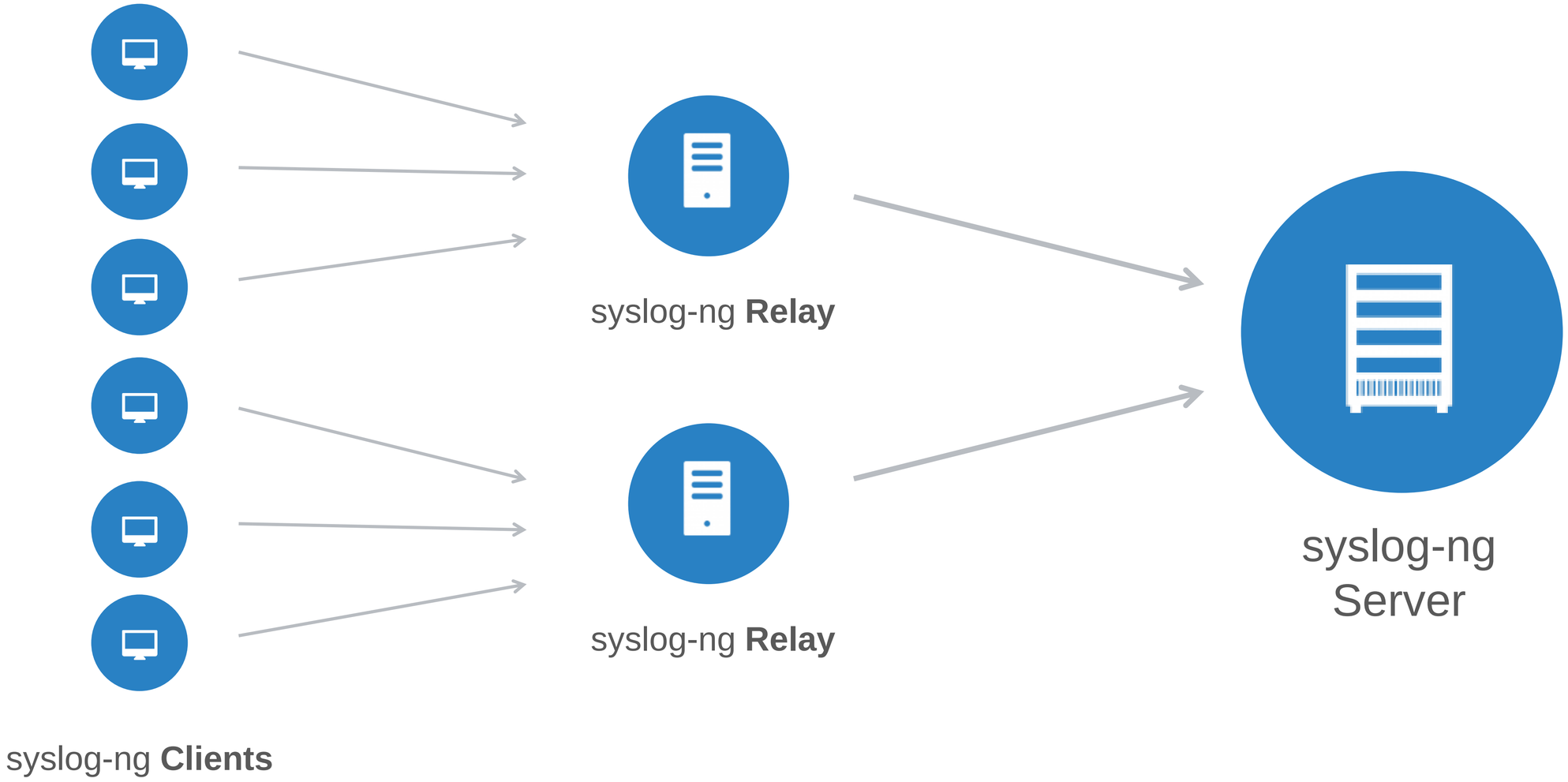
SYSLOG-NG DESCRIPTION



CHALLENGES OF LOG COLLECTION



SYSLOG-NG ARCHITECTURE



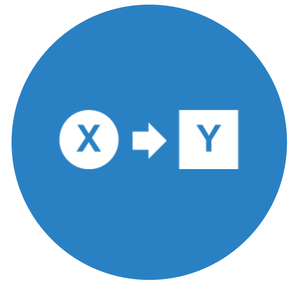
REAL TIME TRANSFORMATION

Filter

Classify

Parse

Rewrite



Normalize

Makes Log Data **Easier to Analyze**

BALABIT

SYSLOG-NG STORE BOX DESCRIPTION

Turnkey solution
Physical / Virtual Appliance

High performance indexing
100,000 logs/sec sustained
35 GB/hr

Web- Based Intuitive GUI
Visualization Statistics

Full text search

Reports

Automated Archiving
Raw storage: 1TB - 10 TB

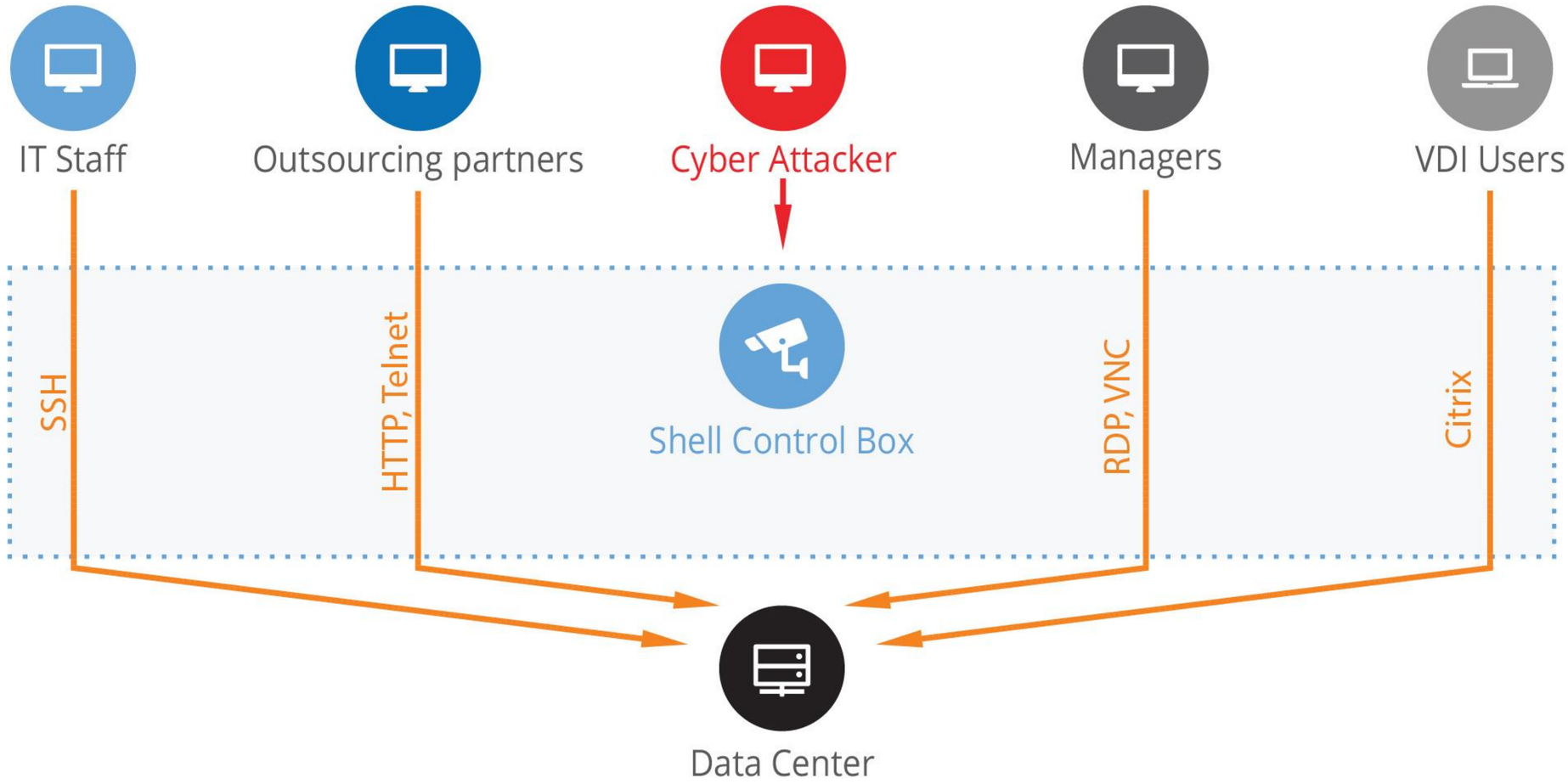
Granular access control
LDAP/Radius Integration

RESTful API

BALABIT

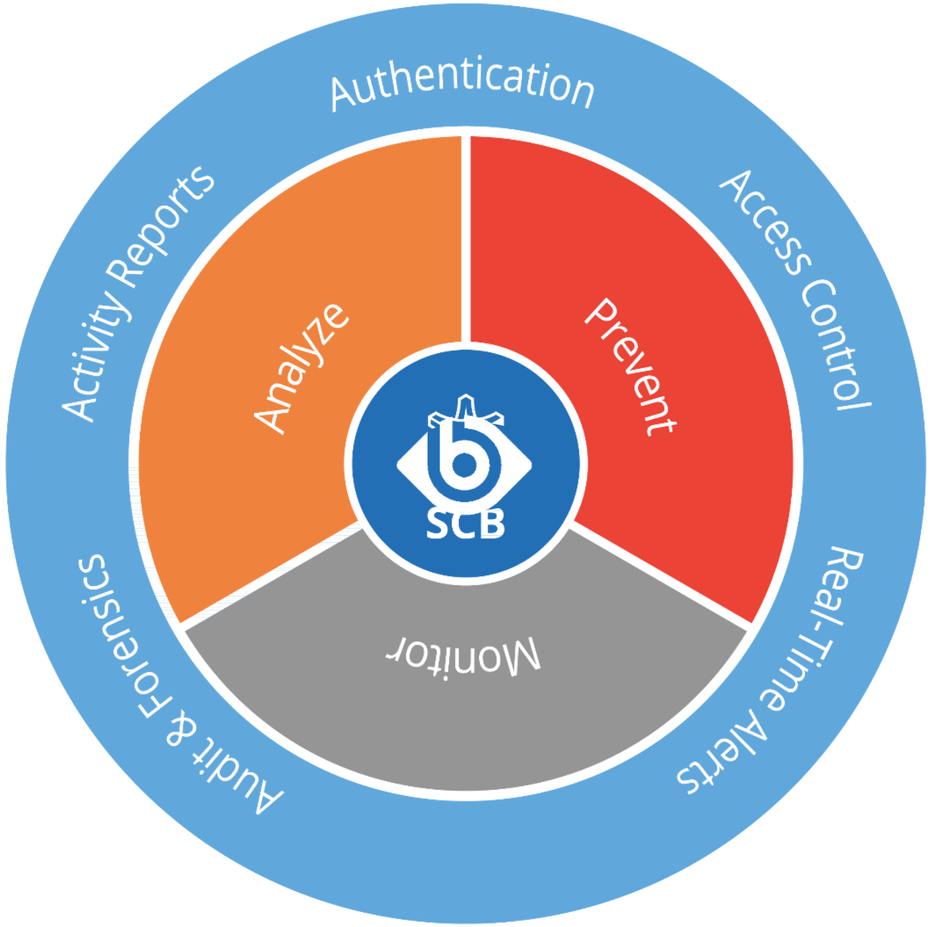
Shell Control Box

High-fidelity recordings: PAM - Shell Control Box

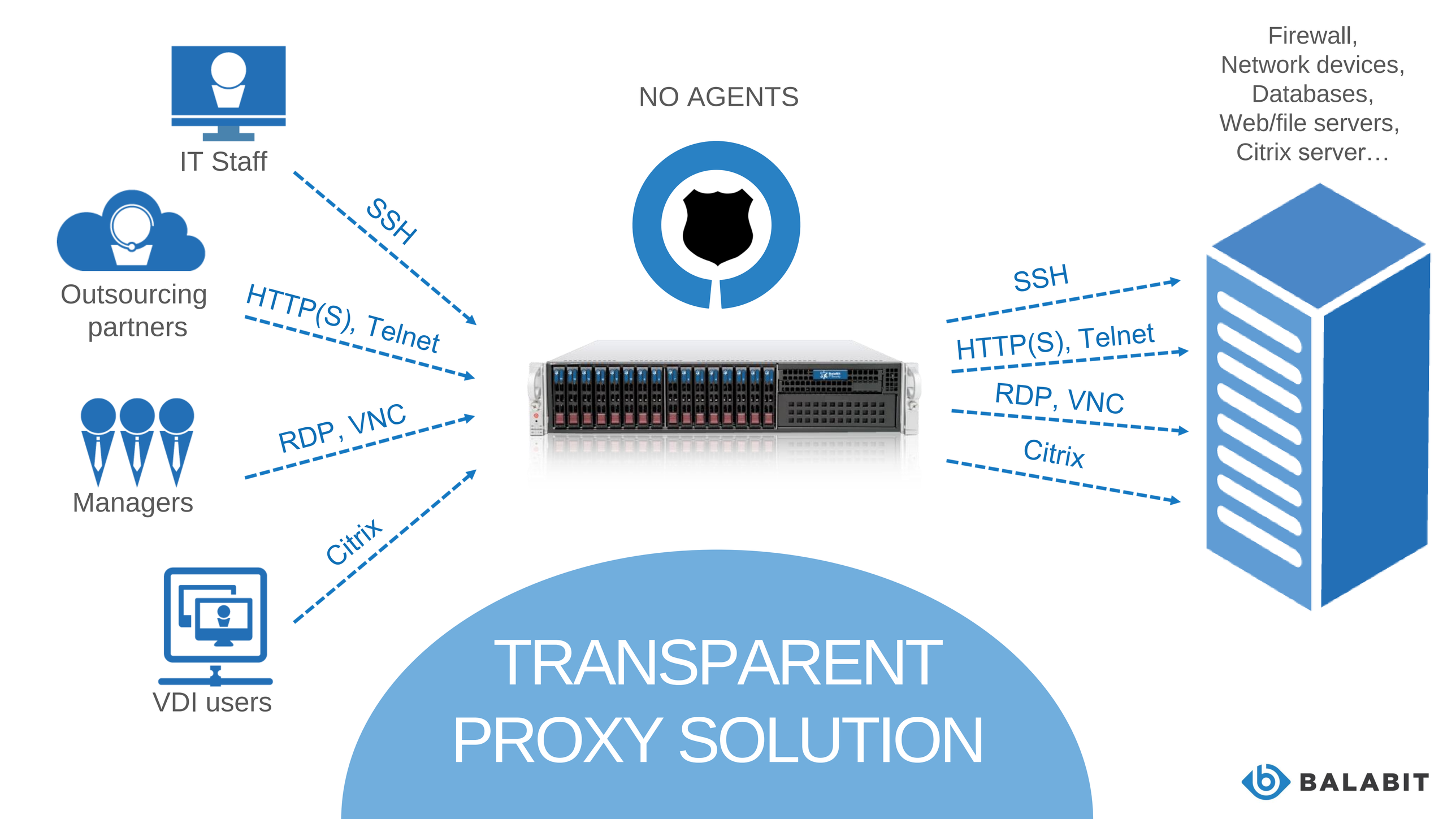


Privileged Activity Monitoring = Immediate Benefits

- Implementation without changing workflows, clients/servers (no agents)
- Augmented log data
- Centralized authentication and authorization
- Credential management
- Audit trails for forensic investigations



BALABIT


IT Staff
Outsourcing partners
Managers
VDI users
SSH
HTTP(S), Telnet
RDP, VNC
Citrix
NO AGENTS
SSH
HTTP(S), Telnet
RDP, VNC
Citrix
Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…
TRANSPARENT
PROXY SOLUTION
BALABIT

IT Staff

Outsourcing partners

Managers

VDI users

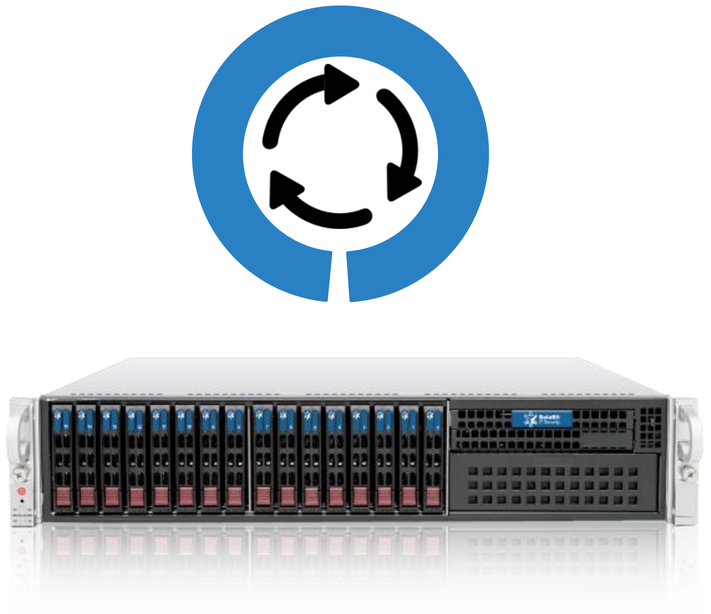
SSH

HTTP(S), Telnet

RDP, VNC

Citrix

USE STANDARD TOOLS



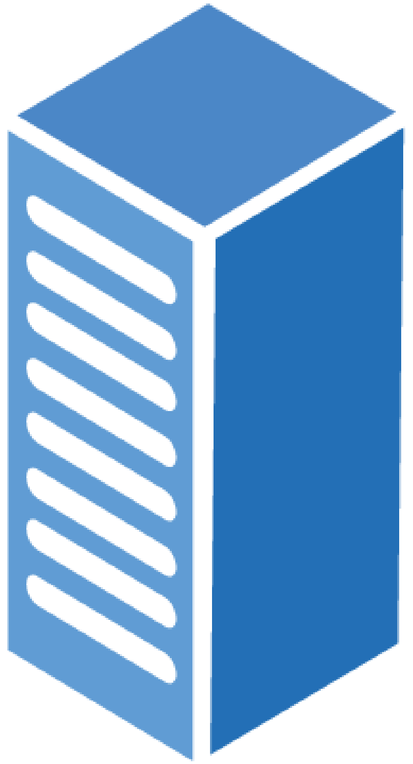
SSH

HTTP(S), Telnet

RDP, VNC

Citrix

Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…



TRANSPARENT PROXY SOLUTION

BALABIT

IT Staff

Outsourcing partners

Managers

VDI users

SSH

HTTP(S), Telnet

RDP, VNC

Citrix

TAMPER-PROOF EVIDENCE

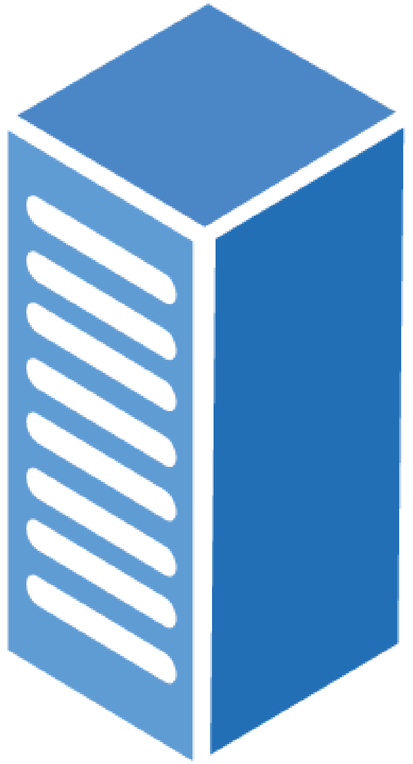
SSH

HTTP(S), Telnet

RDP, VNC

Citrix

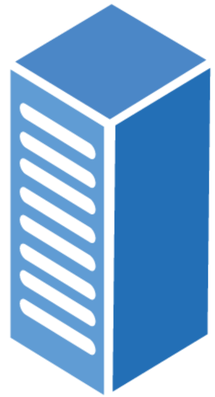
Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…



TRANSPARENT PROXY SOLUTION

BALABIT

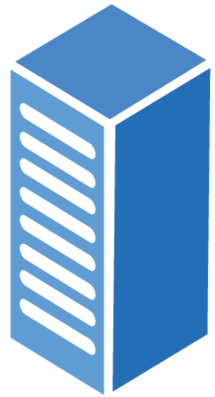
4-eyes Control



Outsourcee

BALABIT

4-eyes Control



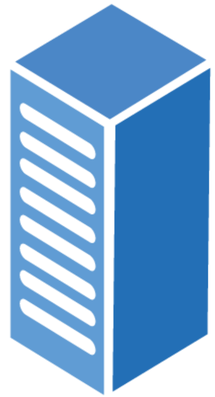
Outsourcee

BALABIT

4-eyes Control

Authorizer

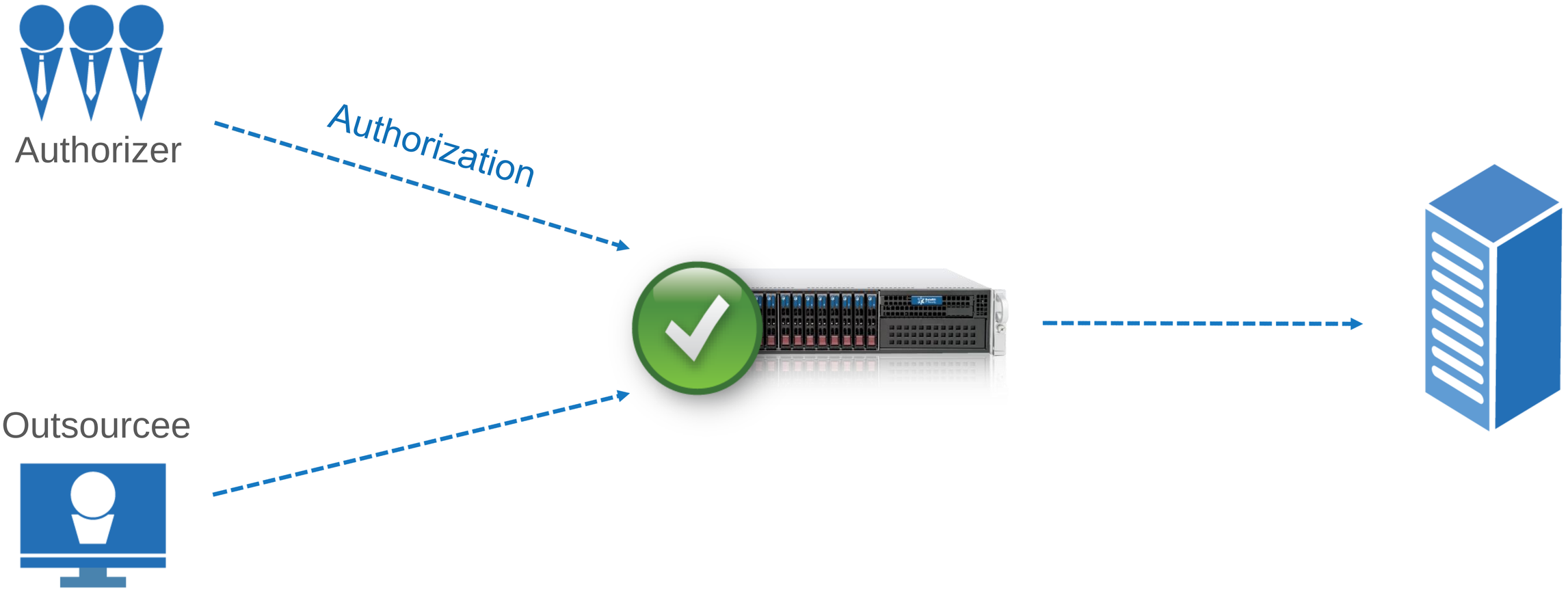
Authorization



Outsourcee

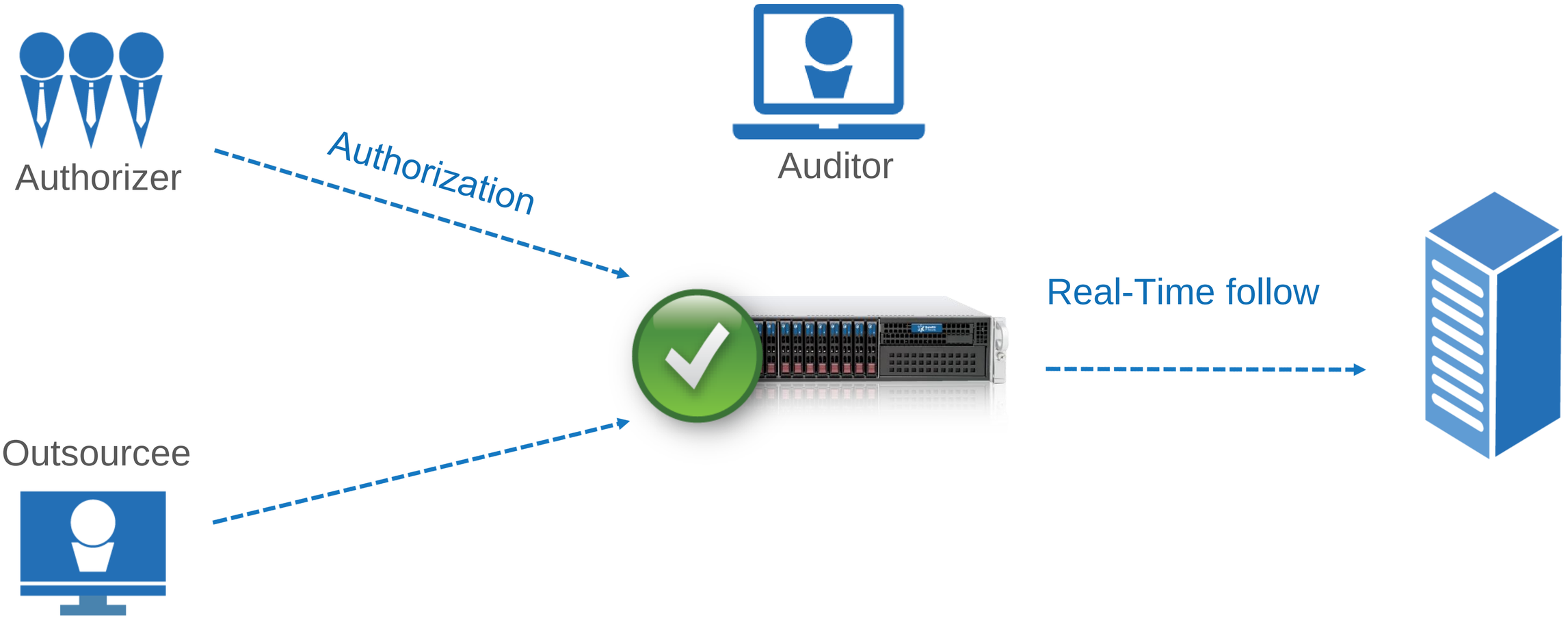
BALABIT

4-eyes Control



BALABIT

4-eyes Control



BALABIT

Real-time Prevention

telnet

SSH

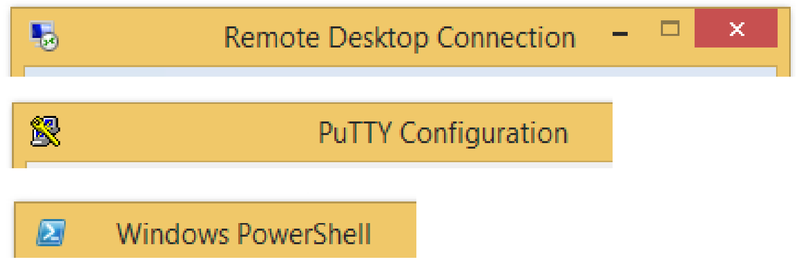
> scp financial.db

Command detection

> cat credit-cards
>1234 5678 9123 4567

Screen-content detection

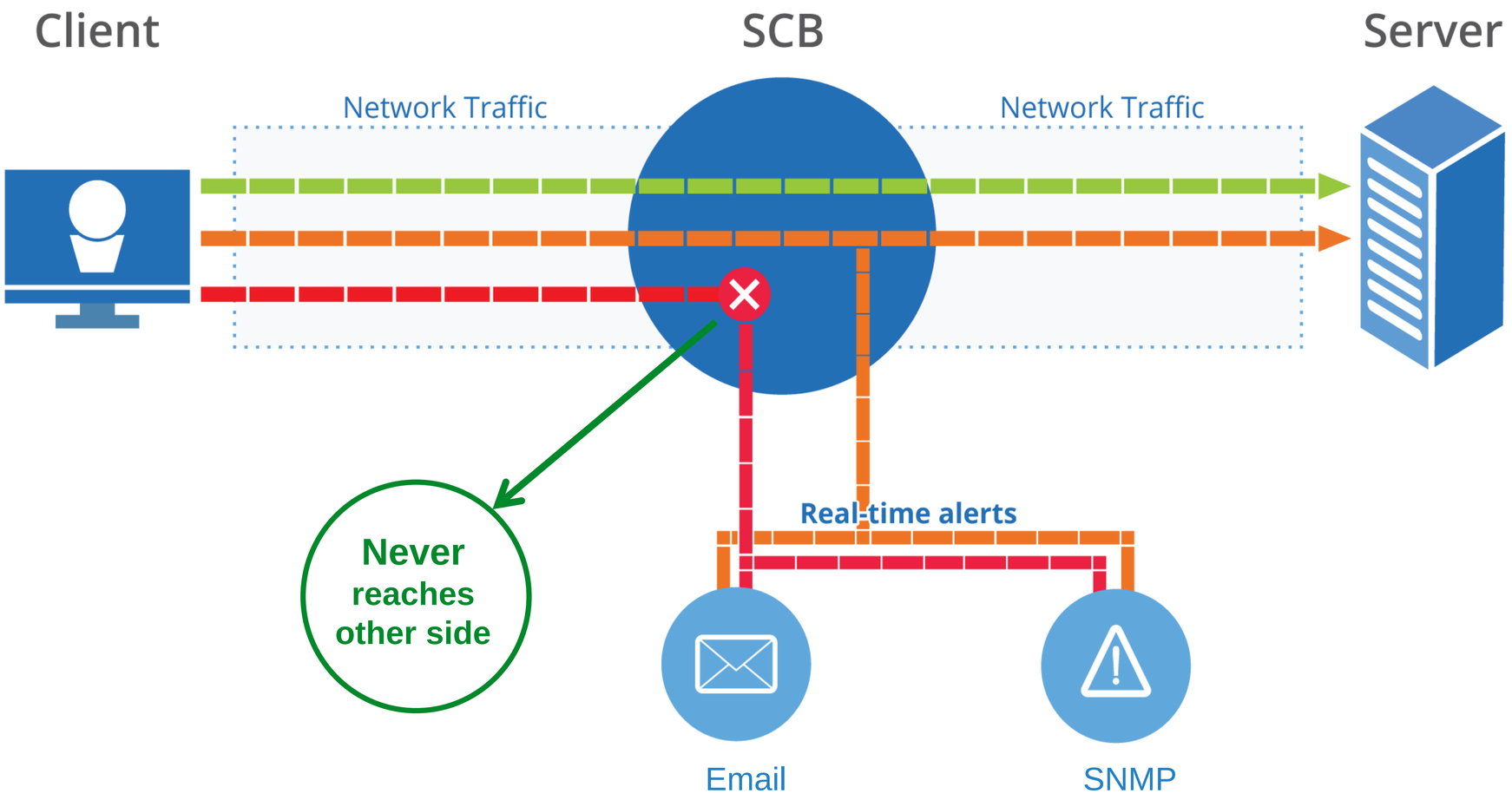
CITRIX



Window-title detection

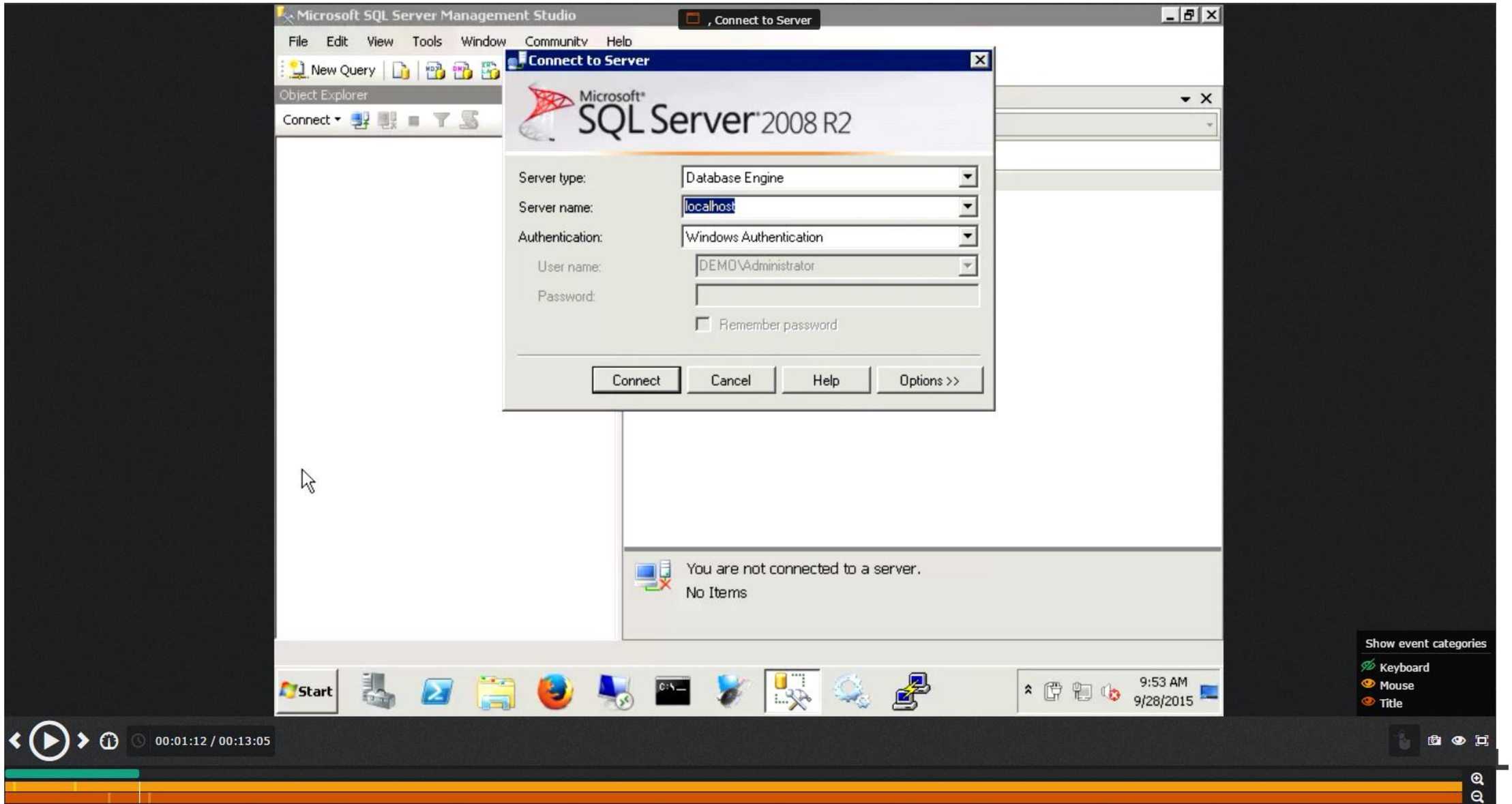
BALABIT

Real-time Prevention



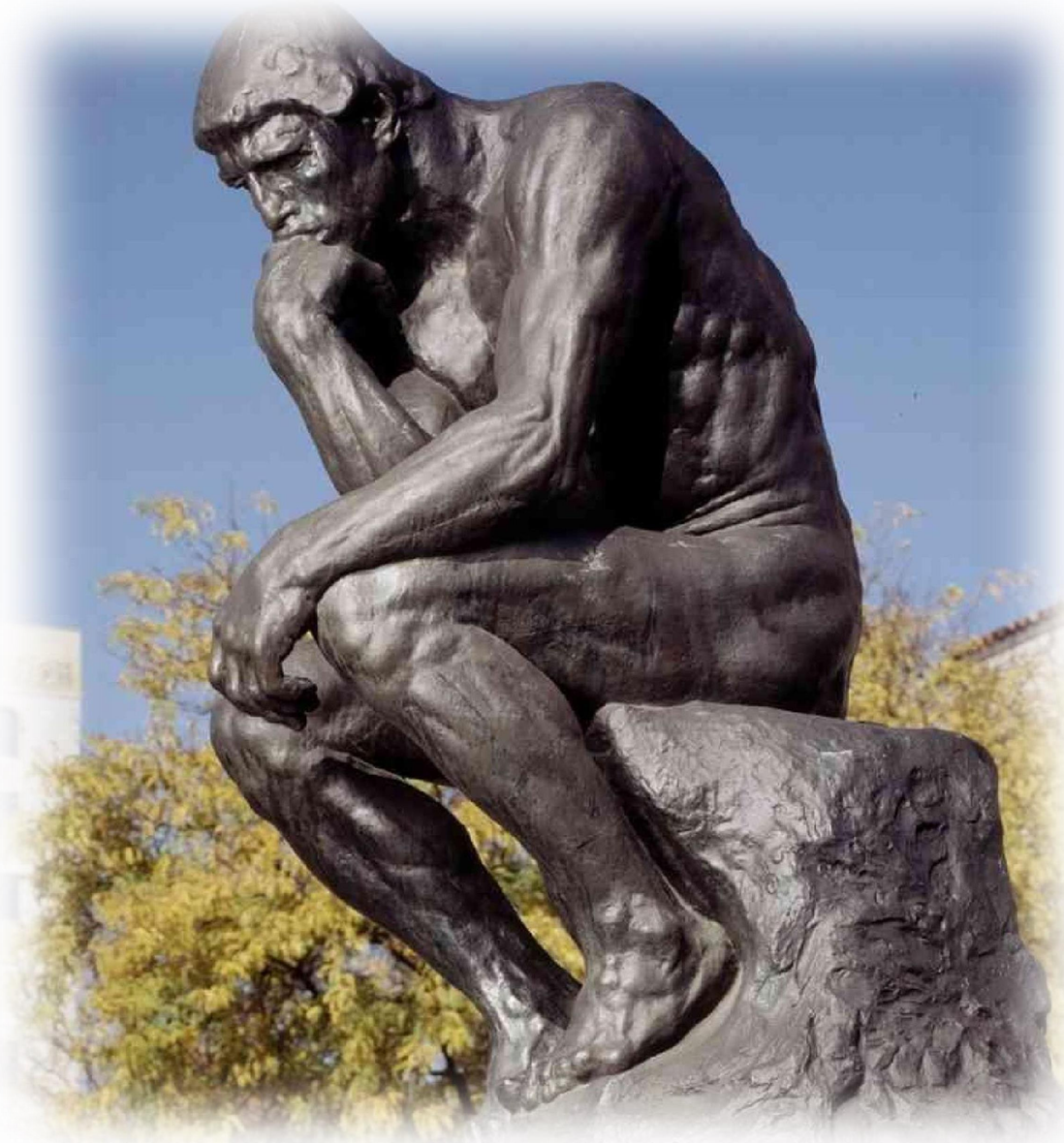
BALABIT

Review of the Audit Trails



Is reliable data enough?

- How do you know when privileged users do something bad?
- Are you sure that your people use their access in a responsible and compliant way?
- Can you hire enough skilled security analysts?
- Are you comfortable with your current method of reviewing logs and auditing records?



BALABIT

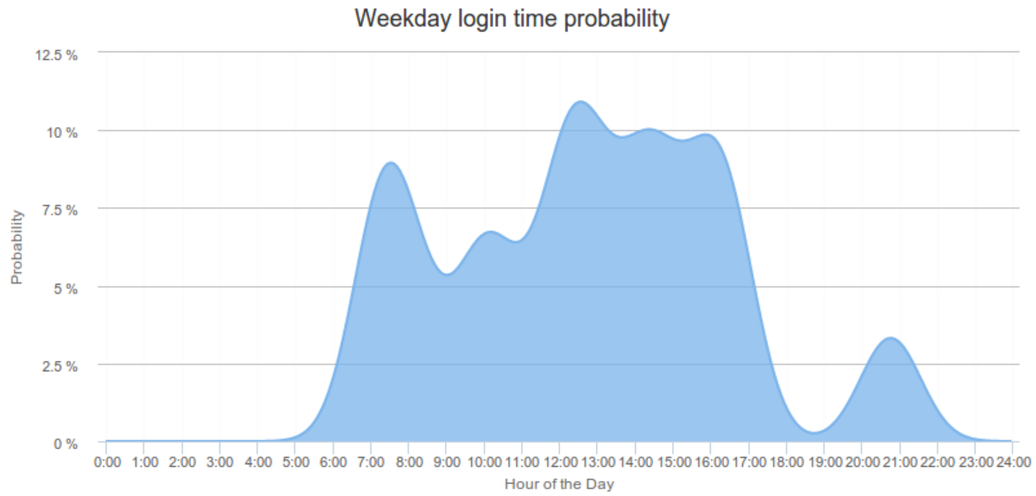
CONTEXTUAL SECURITY INTELLIGENCE

CSI.USER: Understanding the user

Math: no need to reinvent the wheel

Math: no need to reinvent the wheel

- Time distributions – Kernel density analysis



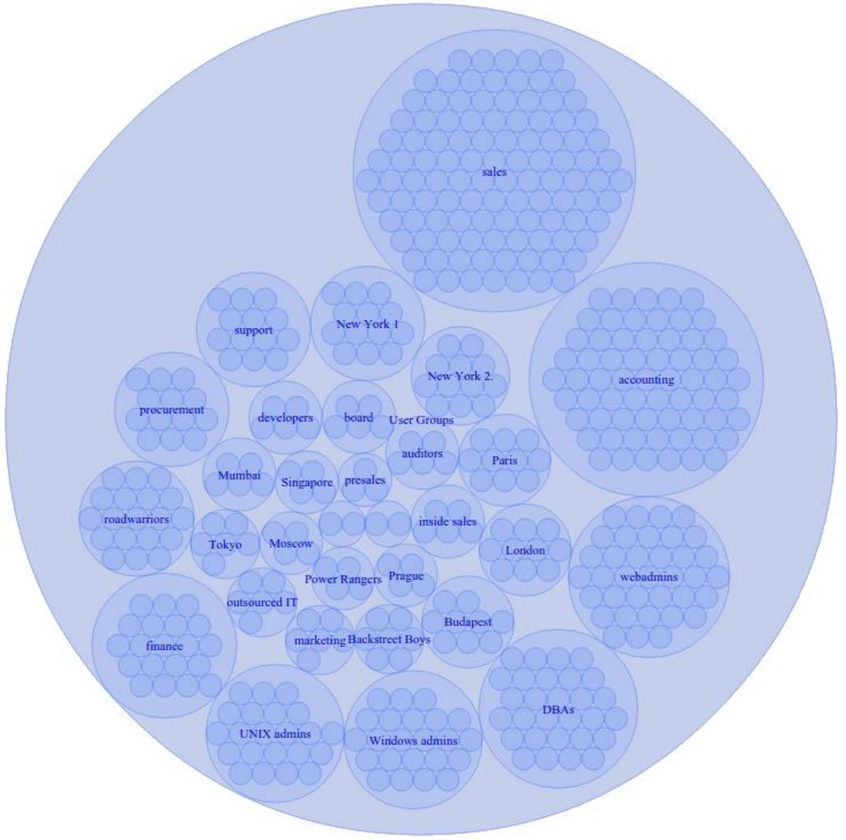
Math: no need to reinvent the wheel

- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining

```
protocol='ssh' port='22' client_ip='192.168.1.1'
protocol='ssh' port='22' client_ip='192.168.1.7'
protocol='ssh' port='22' client_ip='192.168.1.12'
protocol='ssh' port='22' client_ip='192.168.1.32'
protocol='ssh' port='22' client_ip='192.168.1.1'
protocol='ssh' port='1122' client_ip='192.168.1.1'
```

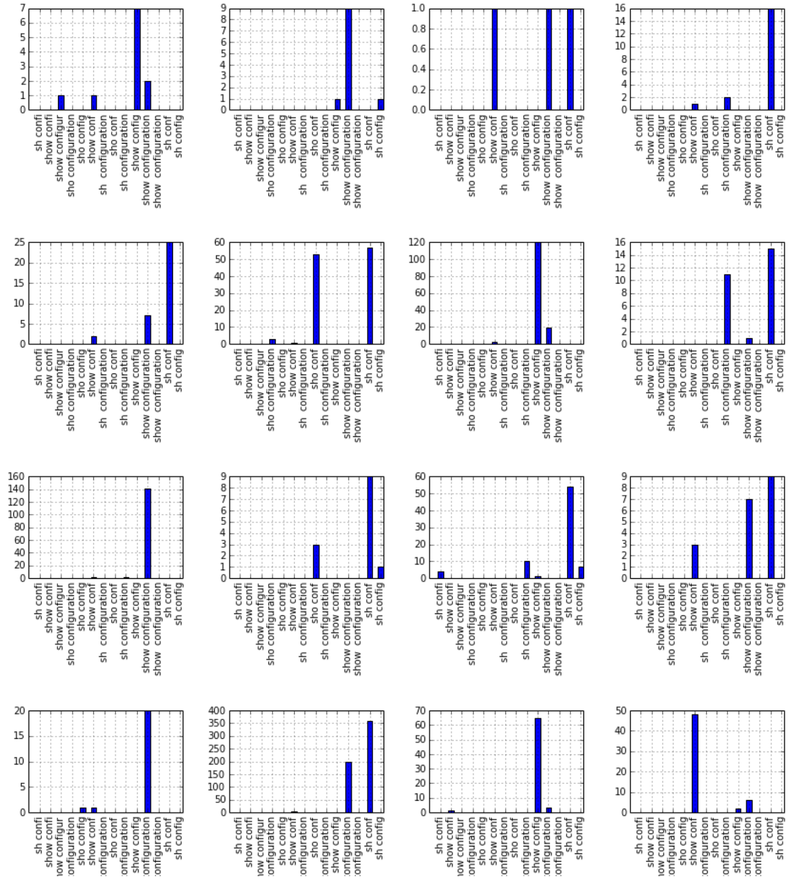
Math: no need to reinvent the wheel

- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining
- Recommender systems & clustering



Math: no need to reinvent the wheel

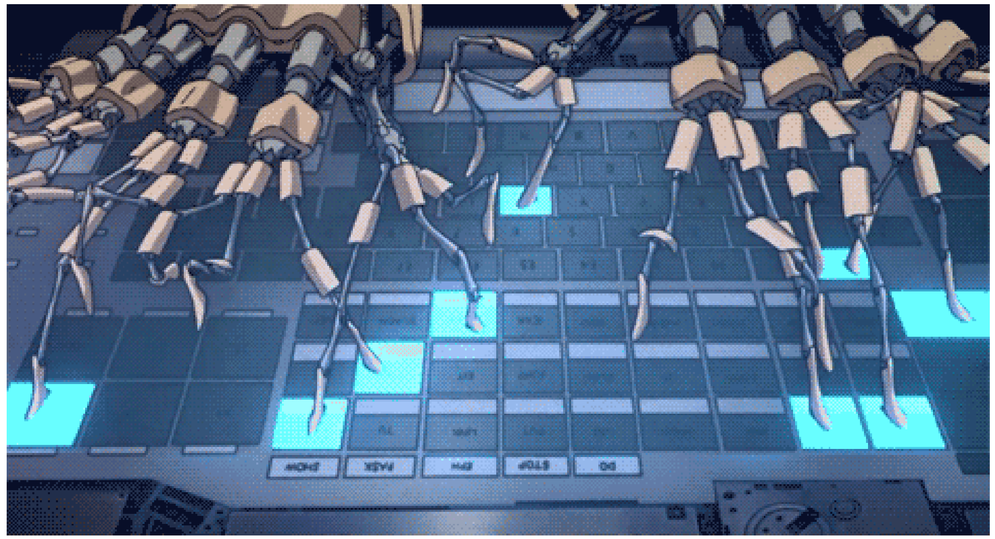
- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining
- Recommender systems & clustering
- Analysis of commands and window titles – Text analysis



BALABIT

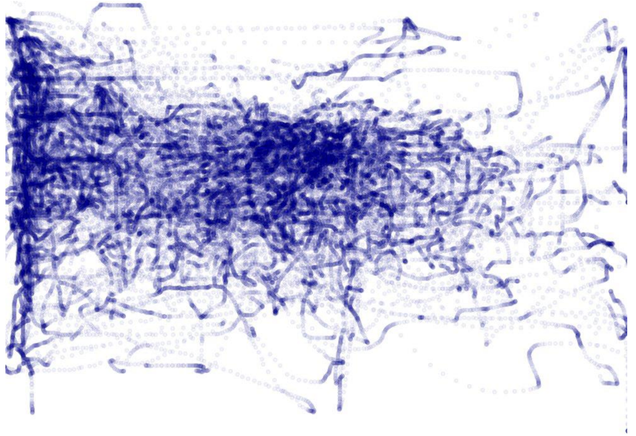
Math: no need to reinvent the wheel

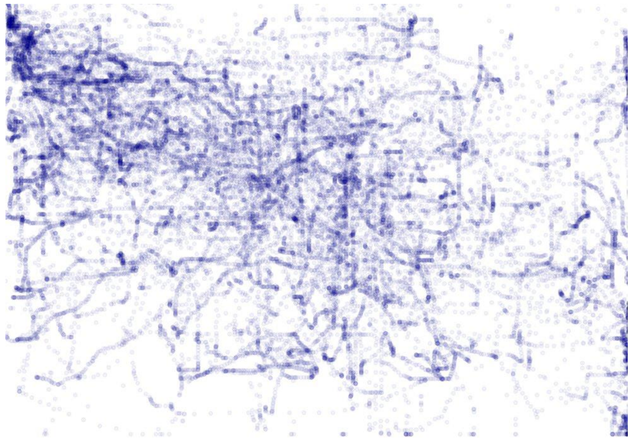
- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining
- Recommender systems & clustering
- Analysis of commands and window titles – Text analysis
- Keystroke dynamics – Stochastic outlier selection



Math: no need to reinvent the wheel

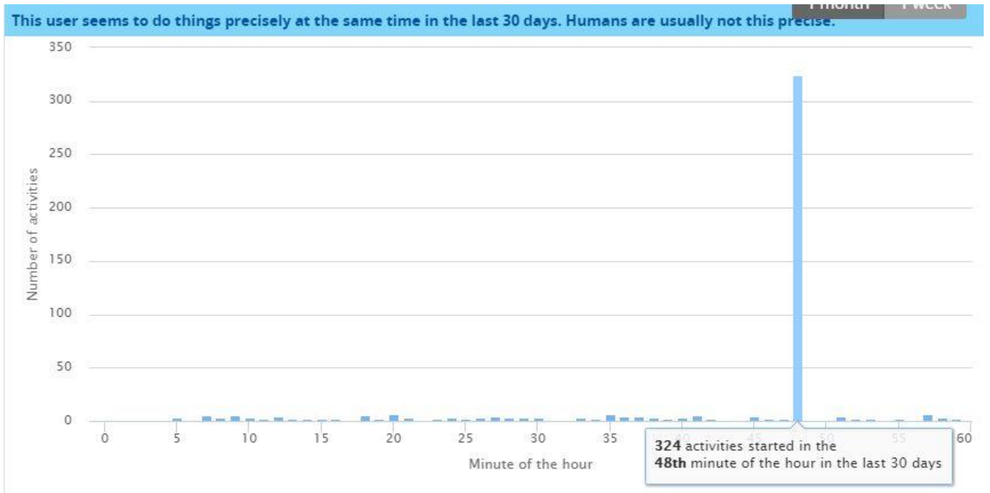
- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining
- Recommender systems & clustering
- Analysis of commands and window titles – Text analysis
- Keystroke dynamics – Stochastic outlier selection
- Pointing device detection – Supervised machine learning on mouse gestures





Math: no need to reinvent the wheel

- Time distributions – Kernel density analysis
- Association rule learning – Frequent itemset mining
- Recommender systems & clustering
- Analysis of commands and window titles – Text analysis
- Keystroke dynamics – Stochastic outlier selection
- Pointing device detection – Supervised machine learning on mouse gestures
- Scripted account detection – Statistical hypothesis testing of periodicity



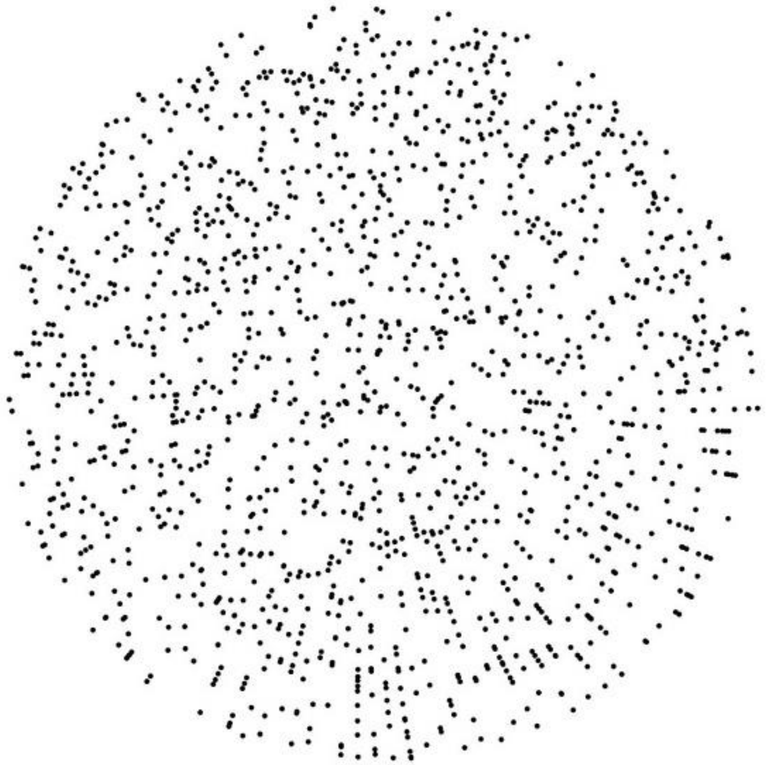
BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

CSI.RISK: Identifying risk

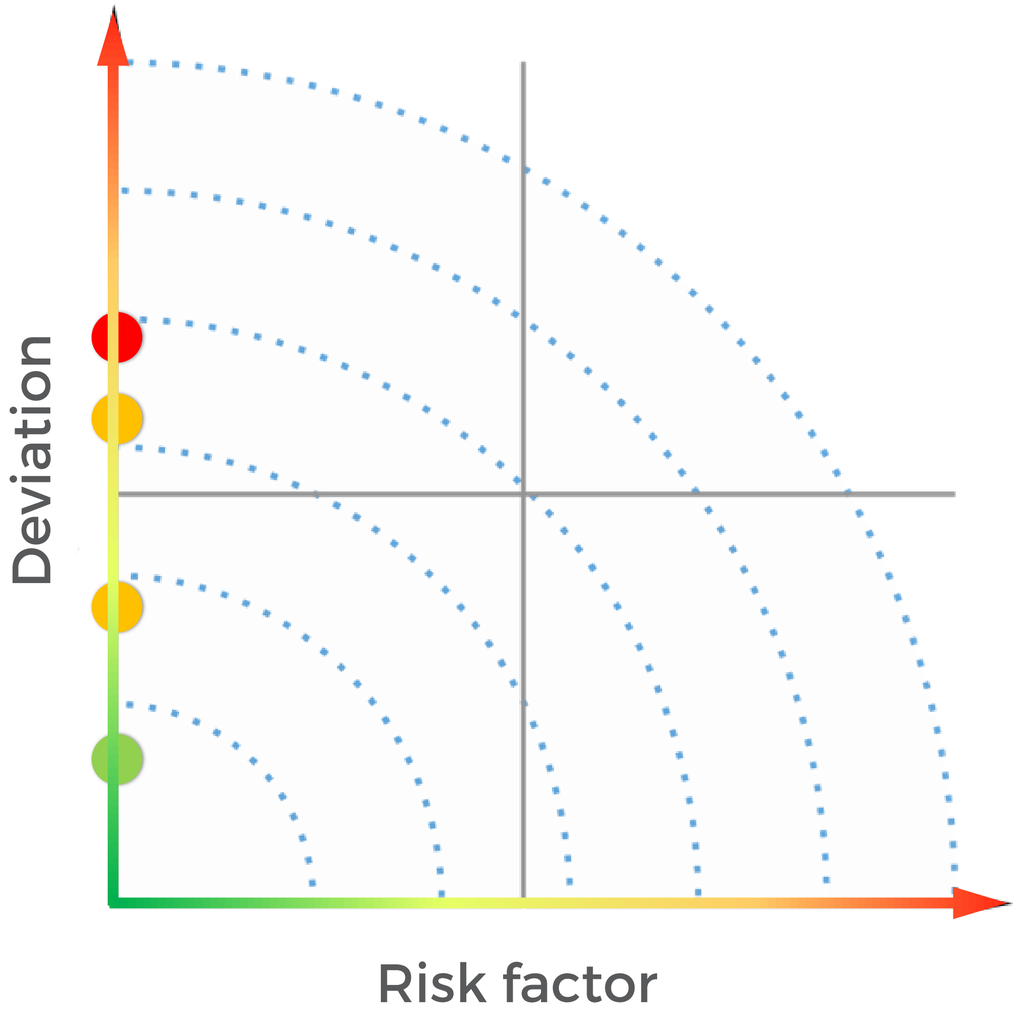
How to Review?

- Which part of the audit trails are the most interesting?
- How to choose which vendors should be reviewed?
- Which solution is significantly better than random sampling?



BALABIT

Focus on the important



- DBA runs a query on the customers' table
- DBA restarts Oracle
- Trainee logs in at 11PM
- Trainee logs in at 9AM

Priority list based on risk factor and deviation

How about cheating them?

BALABIT

Cheating machine learning algorithms

- Cheating ONE algorithm requires:
  - A valid user credential
  - Perfect knowledge about the selected algorithm
  - Time
- Cheating ALL algorithms requires:
  - Several valid user credentials
  - Perfect knowledge about ALL of the algorithms in Blindspotter
  - Really lot of time – even years

…and peer group analysis may be able to find this anomaly as well

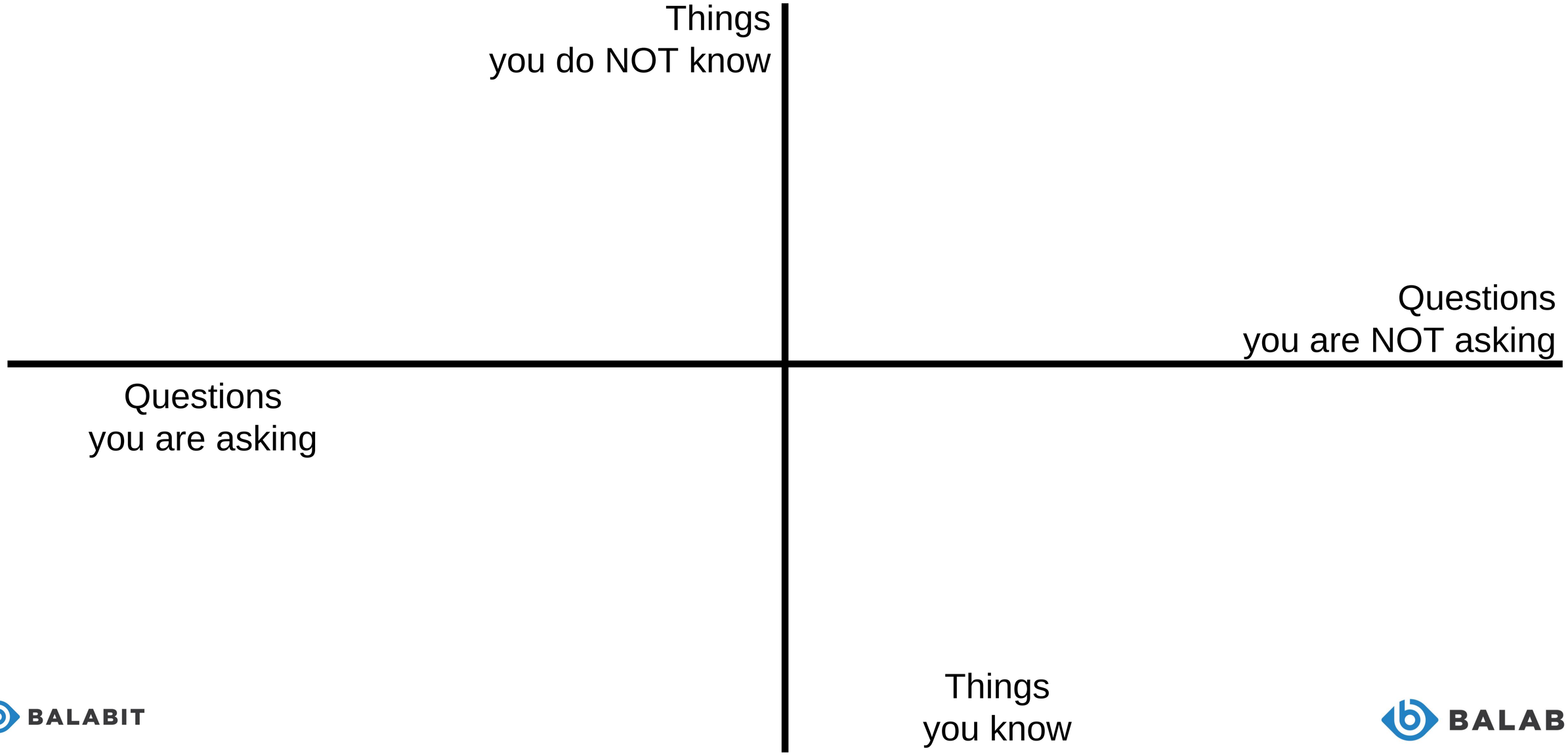
What is Behavior?

”Behavior is the internally coordinated responses of whole living organisms to internal and/or external stimuli”

Daniel A. Levitis, PhD in Integrative Biology

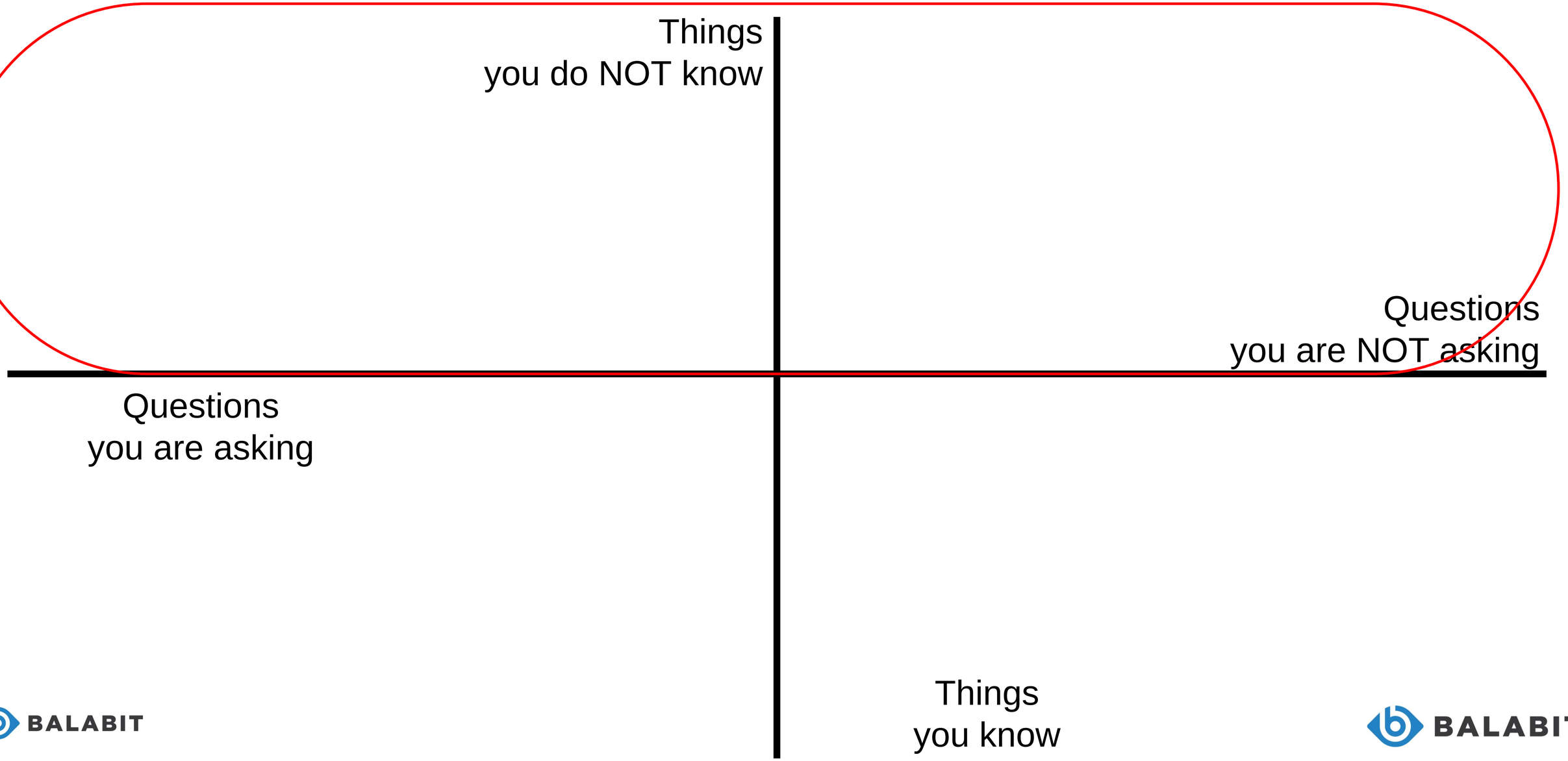
BALABIT

0-knowledge Threats



BALABIT

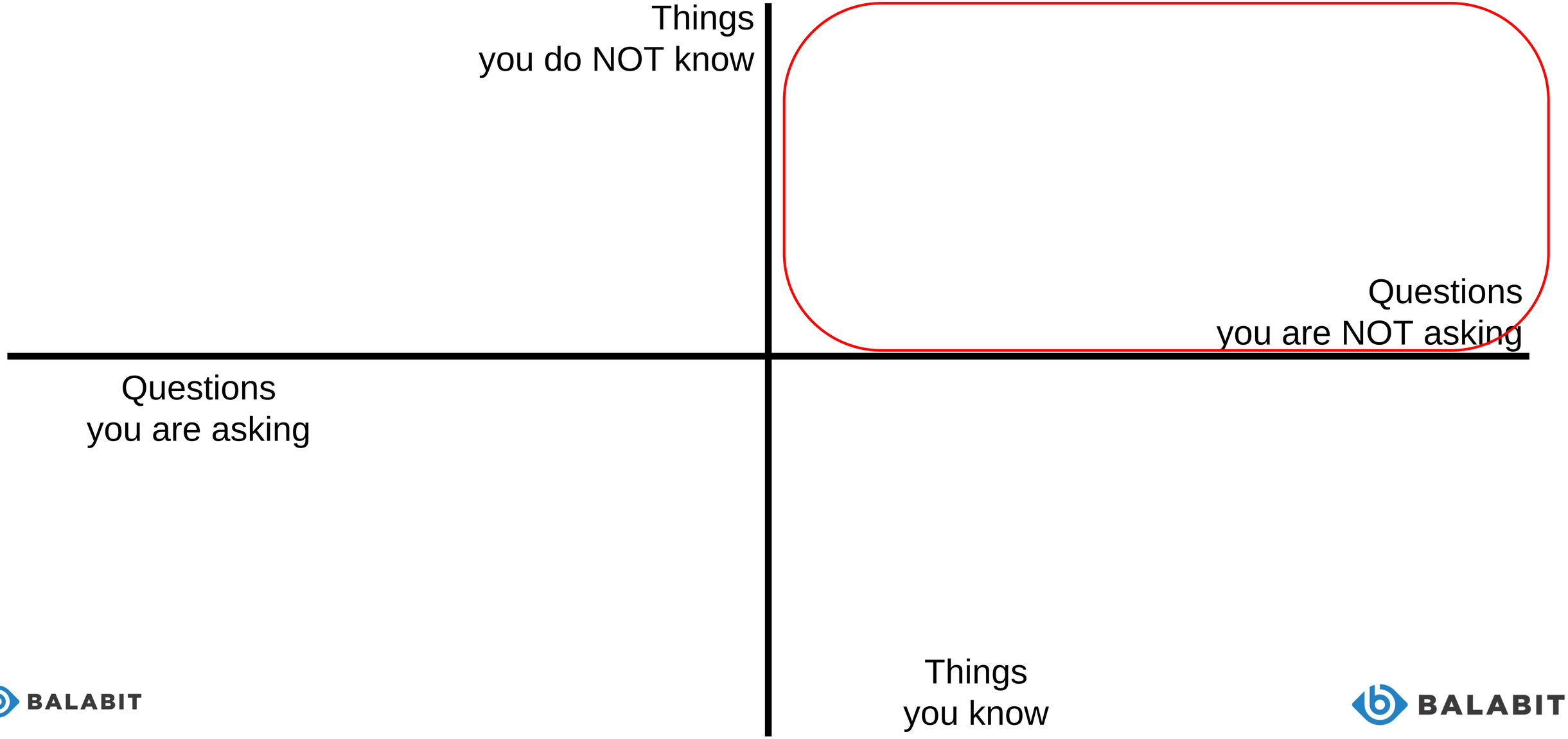
0-knowledge Threats



BALABIT

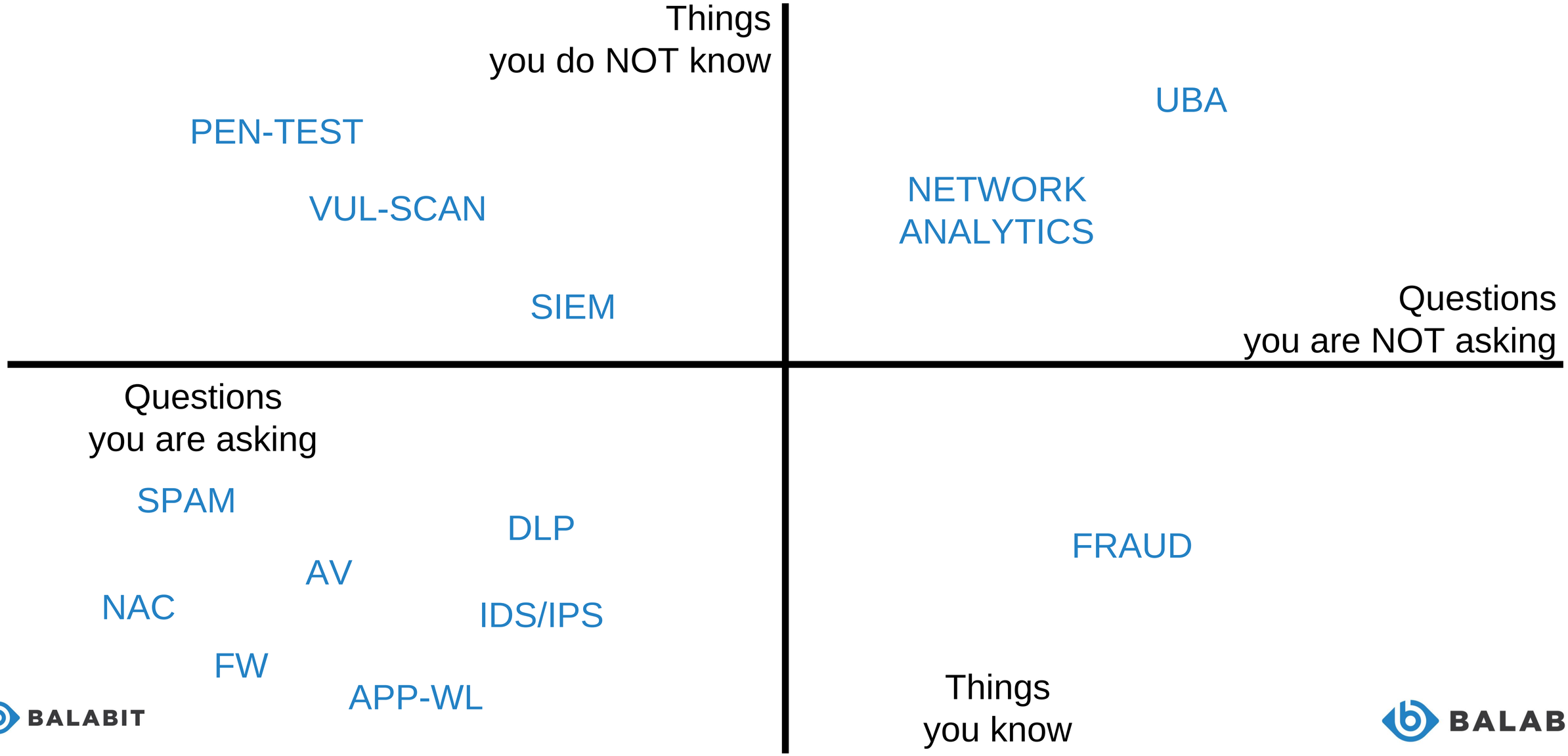
BALABIT

0-knowledge Threats



BALABIT

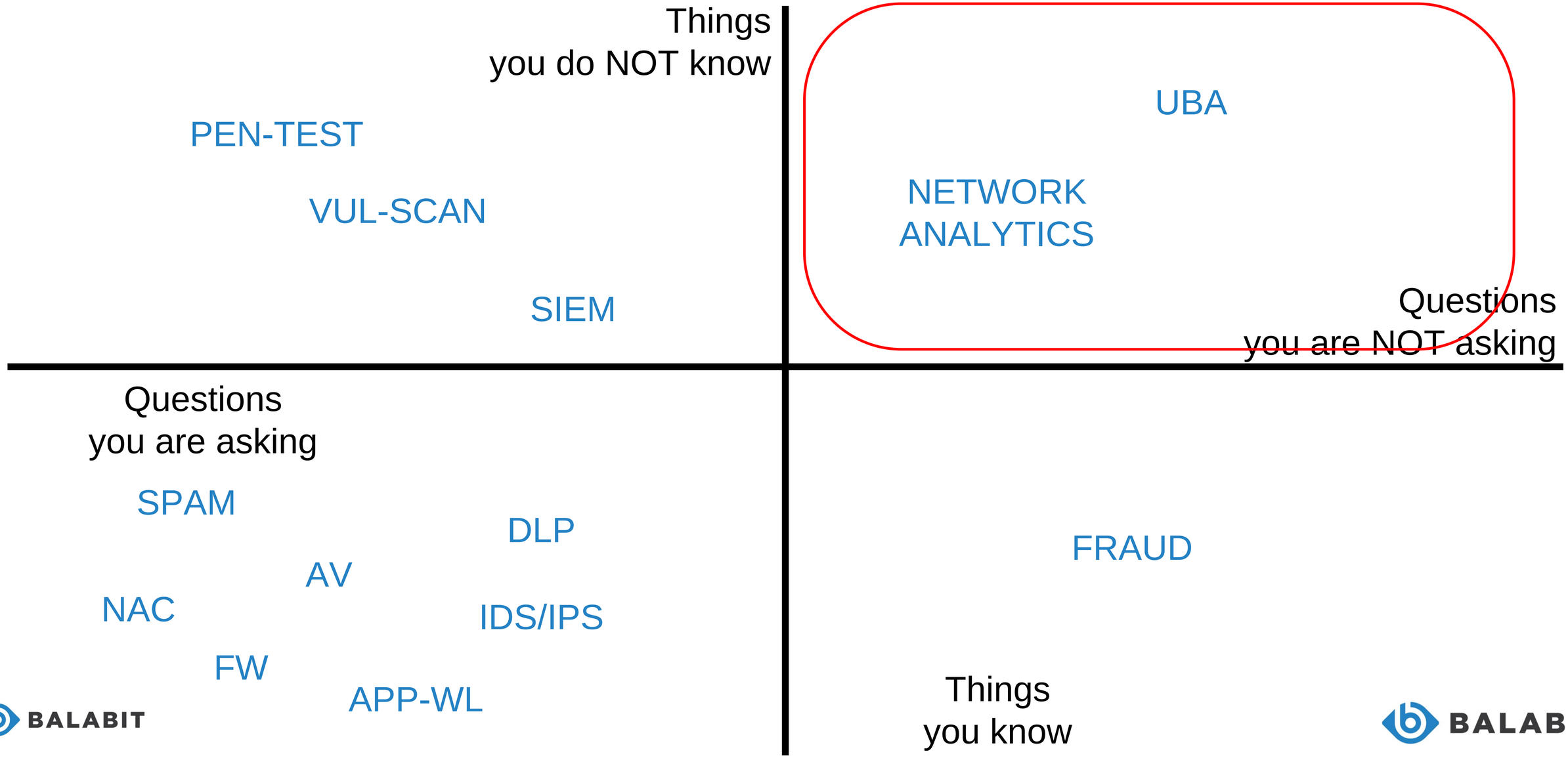
0-knowledge Threats



BALABIT

BALABIT

0-knowledge Threats



BALABIT

BALABIT

HOW IS CSI DIFFERENT?

Traditional security approach

Contextual security approach

BALABIT

HOW IS CSI DIFFERENT?

Traditional security approach	Contextual security approach
Manually defined	Self learning

HOW IS CSI DIFFERENT?

Traditional security approach	Contextual security approach
Manually defined	Self learning
Enforcing control	Real-time knowledge & interaction

BALABIT

HOW IS CSI DIFFERENT?

Traditional security approach	Contextual security approach
Manually defined	Self learning
Enforcing control	Real-time knowledge & interaction
Security damages continuity	More Security with more freedom

BALABIT

HOW IS CSI DIFFERENT?

Traditional security approach	Contextual security approach
Manually defined	Self learning
Enforcing control	Real-time knowledge & interaction
Security damages continuity	More Security with more freedom
ROI only when attacked	Immediate visibility of ROI

BALABIT

HOW IS CSI DIFFERENT?

Traditional security approach	Contextual security approach
Manually defined	Self learning
Enforcing control	Real-time knowledge & interaction
Security damages continuity	More Security with more freedom
ROI only when attacked	Immediate visibility of ROI
Partial vision	Full knowledge of all actions

BALABIT

Thank you for your attention!

Gabor Illes – Presales Engineer
gabor.illes@balabit.com

Q & A