Getting Better Sleep With Analytics-Driven Identity Data Management

Sebastien FAIVRE

CTO

RADIANT LOGIC

The current situation...

90% of former employees retain access to applications more than three months after their departure

43% of terminated accounts are still in use

210: average number of days a hacker is present in the computer systems before attacking

74% of organizations who fell victim to cyberattacks identify over-privileged access as a main cause

26% of security incidents come from internal threats

How did we get here?

Expectations

Bi-directional connectors

Bi-directional connectors

Role model Bi-directional connectors

IGA Platforms

Access control	Self Service	Audit & Reporting	Role Model	Synchronization
	Delegated administration	Dashboard	Compliance Controls	Integration Service
	Help Desk	SoD controls	Directory Services	Lifecycle Workflows
	Access Request	Access Review	Policy Management	Notification
Identity Warehouse (Repository)		Provisioning account & access		Reconciliation

Reality

HR resources

Data feed connector

Active Directory

Bi-directional connectors

Only a few Applications

Role model Bi-directional connectors

Some more Applications

ITSM tickets or emails

All the rest...

Out-of-scope

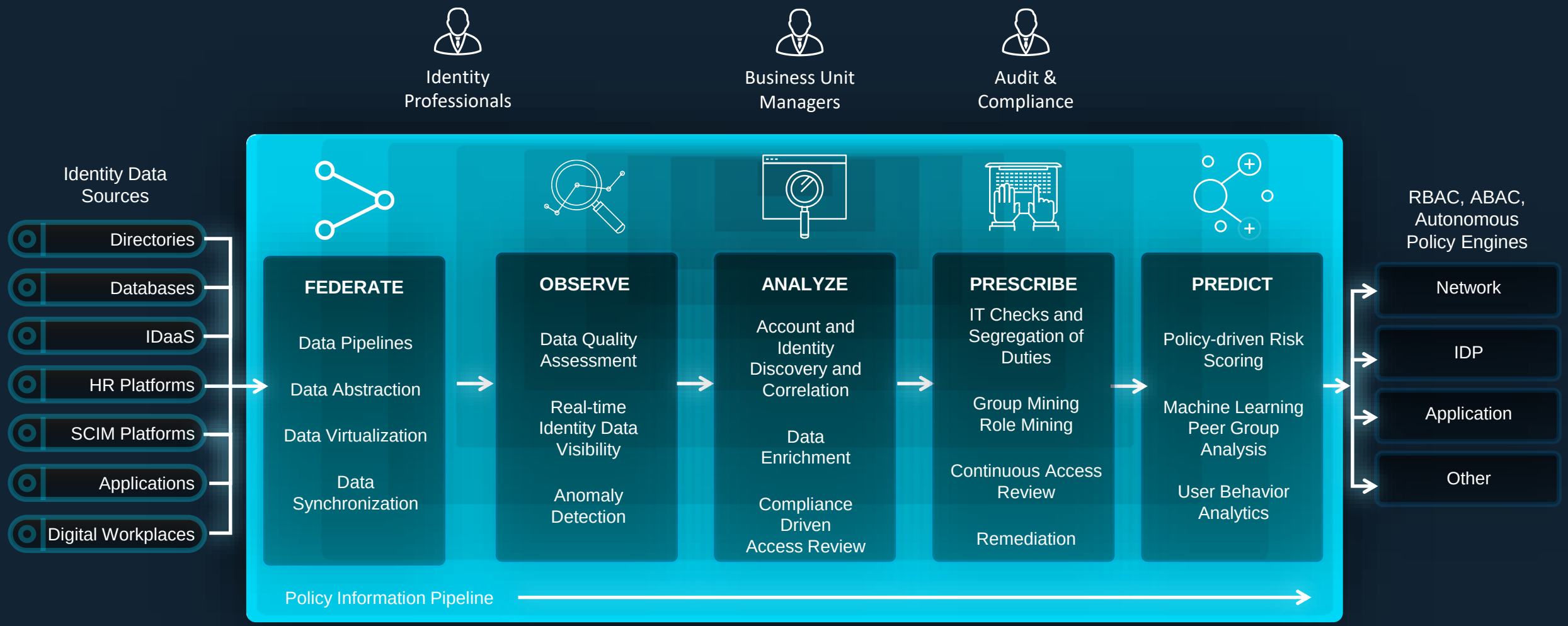
IGA Platforms

Access control	Self Service	Audit & Reporting	Role Model	Synchronization
	Delegated administration	Dashboard	Compliance Controls	Integration Service
	Help Desk	SoD controls	Directory Services	Lifecycle Workflows
	Access Request	Access Review	Policy Management	Notification
Identity Warehouse (Repository)		Provisioning account & access		Reconciliation

Identity is everywhere:

How to tame the Identity problem?

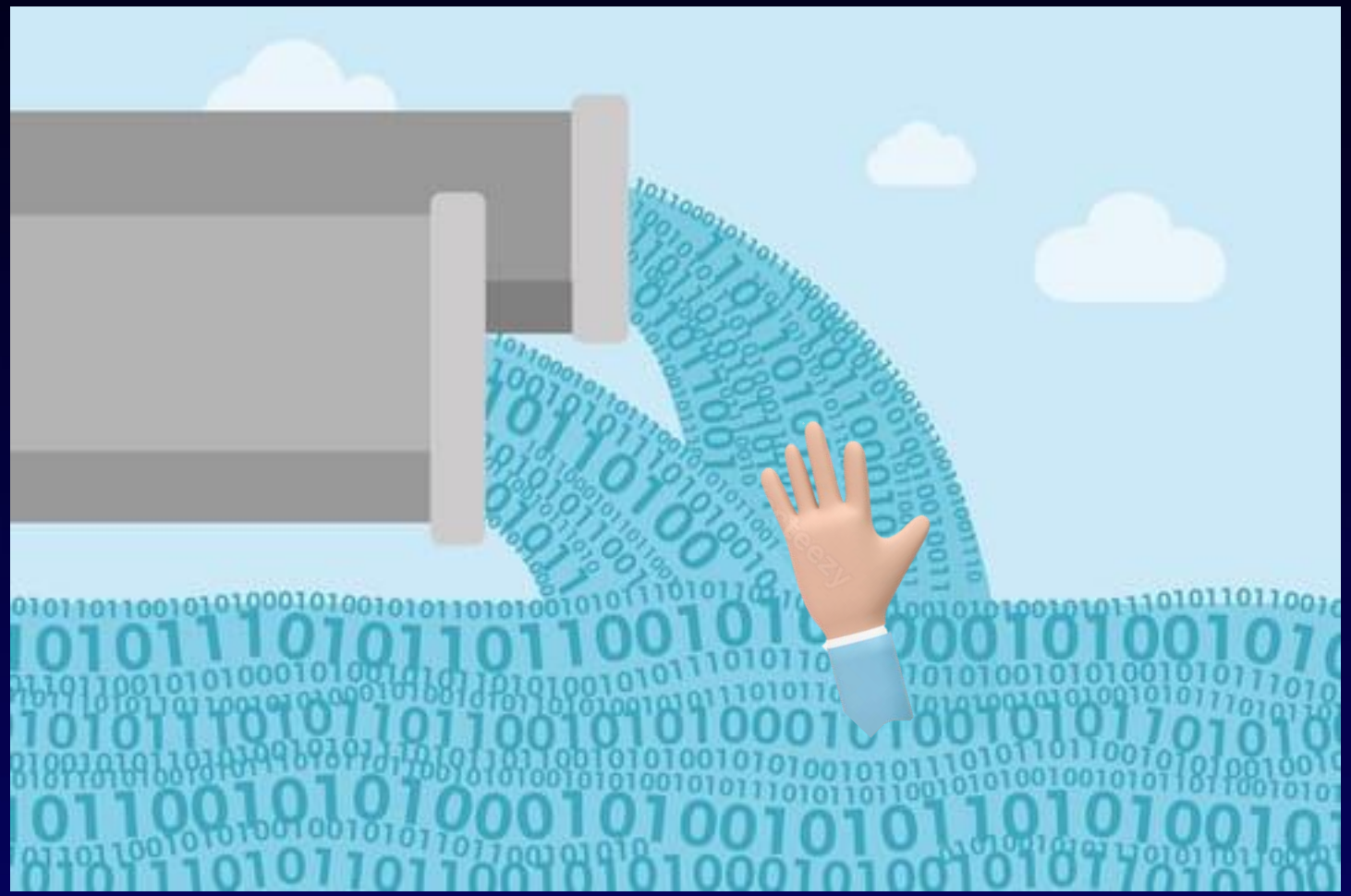
A Proven Framework for Identity-First Security



Common pitfalls and misconceptions

Observe and Analyze

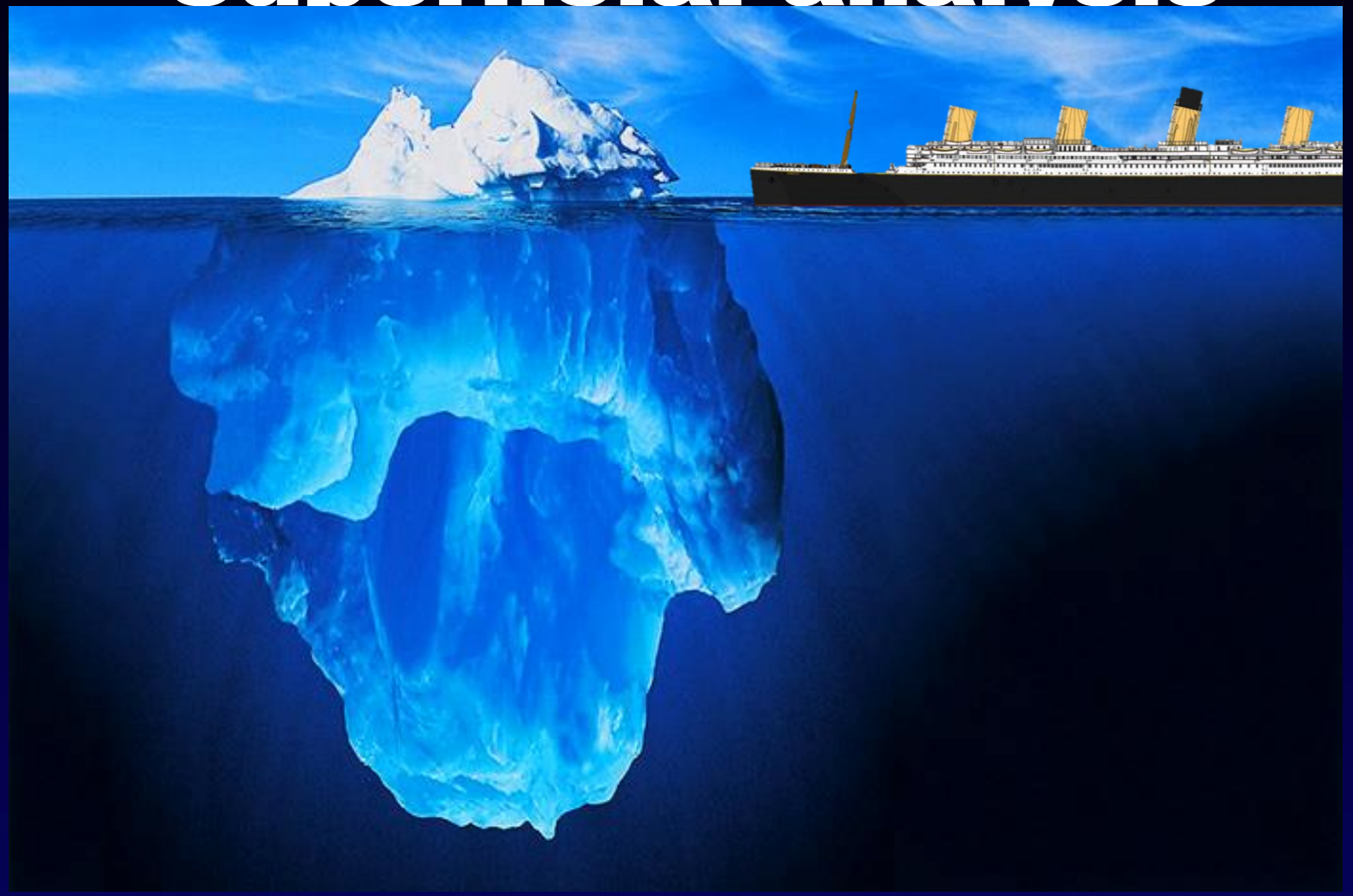
Analysis pitfall
Data accumulation is not insight



Analysis pitfall
Mixing apples and oranges

Analysis pitfall
Missing context

Analysis pitfall
Superficial analysis

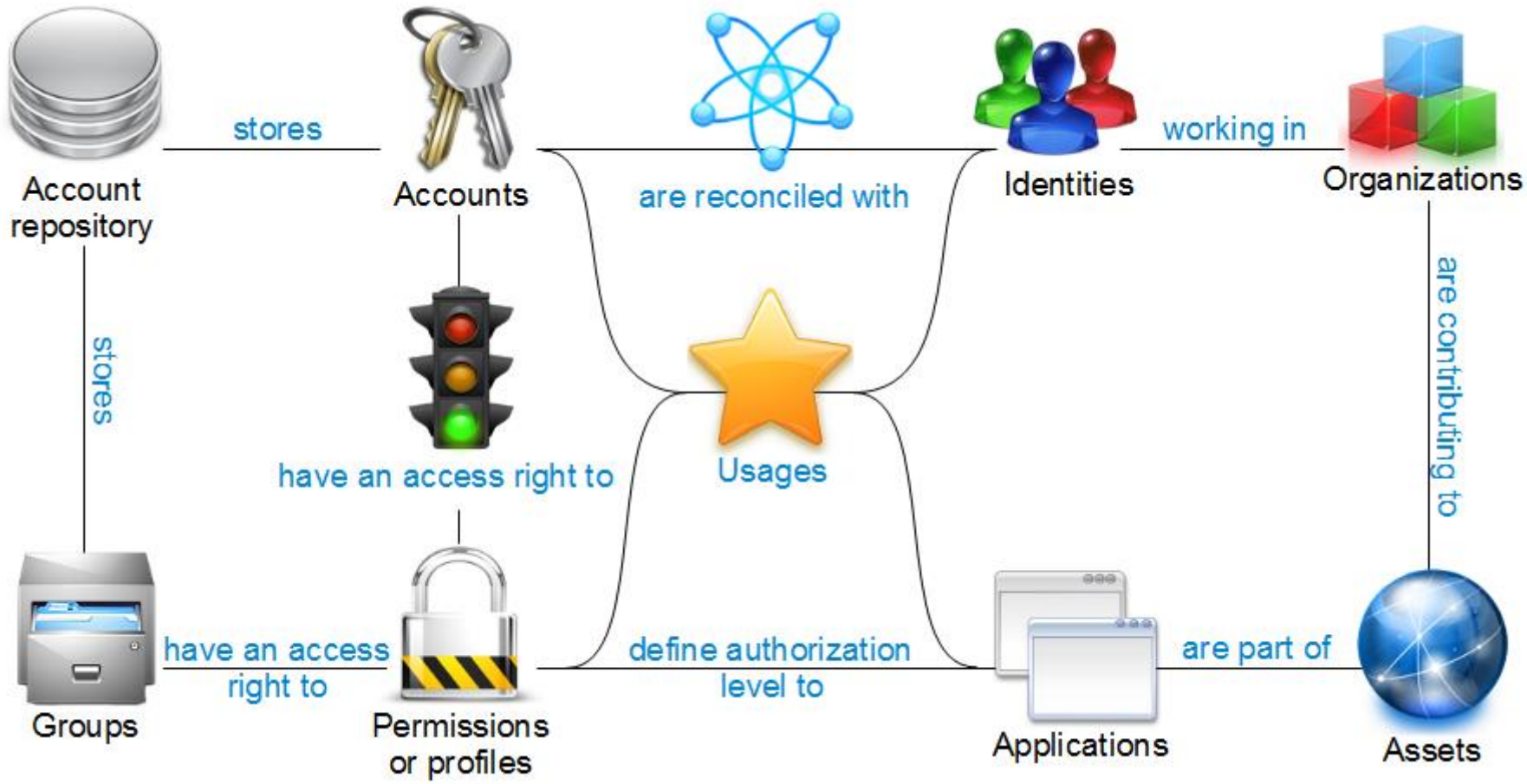


How To Transform Your Identity Data Into Information Business People Can Understand

Aggregation Alone is Not Enough!

Build and fulfill an **Identity and Entitlement data model** instead:

- Correlate the datasources, map them in the data model, and build missing links
- Transform data into meaningful information


Account repository
stores
Accounts
are reconciled with
Identities
working in
Organizations
stores
have an access right to
Usages
are contributing to
Groups
have an access right to
Permissions or profiles
define authorization level to
Applications
are part of
Assets

Data Visualization Techniques To Find the Needle In the the Access Haystack

The Problem...

350,000 Identities

2,000,000 User and Technical Accounts

500,000 Groups

800 Applications...

20,000,000 Access Rights

Data Quality: Orphan Accounts

BRAINWAVE GRC | Identity Analytics Platform | JAIME ROBERTSON

Administrator Home Page

You have 112 remediations to launch

What do you want to explore?

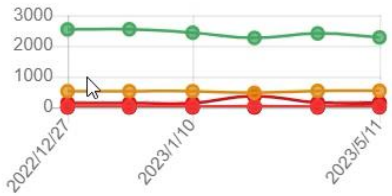
- Browse org. chart
- Search for identities
- Search for organisations
- Search for accounts
- Search for groups
- Search for repositories
- Search for applications
- Search for permissions
- Search for shares
- Search for shared folders
- Search for servers

What do you want to do?

Number of accounts per risk level

Number of identities per risk level

Accounts risk level - Trends



Top 10 risked entities

Top 10 most risky accounts	Top 10 most risky identities	Top 10 most risky organisations
edwin.chandler@acme.com (ACME.COM)	Olive NGUYEN (ID0000112)	France Prospecting Service
lionel.hayes@acme.com (ACME.COM)	Jerome CARLSON (ID0000025)	Cash Management
veronica.hill@acme.com (ACME.COM)	Annie SALAZAR (ID0000030)	Events
patricia.james@acme.com (ACME.COM)	Irvin LLOYD (ID0000427)	Taxes
WDAGUtilityAccount (DC-ACMEPRD.acme.corp)	Jodi ROGERS (ID0000454)	Funds Management
Guest (DC01.acme.corp)	Lorena STEVENSON (ID0000022)	Pre-Sales Service France
noel.hogan@acme.com (ACME.COM)	Mabel TURNER (ID0000074)	FP&A
kari.maldonado@acme.com (ACME.COM)	Jill FORD (ID0000158)	Pre-Sales Service Europe
chad.mcbride@acme.com (ACME.COM)	Van SWANSON (ID0000029)	Training
christopher.park@acme.com (ACME.COM)	Luke COLE (ID0000001)	Payroll Service

IT Checks: Identities

BRAINWAVE GRC | Identity Analytics Platform | JAIME ROBERTSON

Administrator Home Page

You have 112 remediations to launch

What do you want to explore?

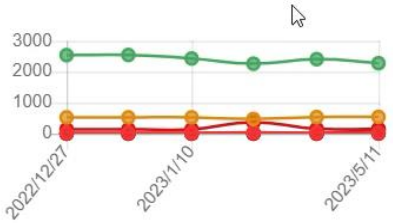
- Browse org. chart
- Search for identities
- Search for organisations
- Search for accounts
- Search for groups
- Search for repositories
- Search for applications
- Search for permissions
- Search for shares
- Search for shared folders
- Search for servers

What do you want to do?

Number of accounts per risk level

Number of identities per risk level

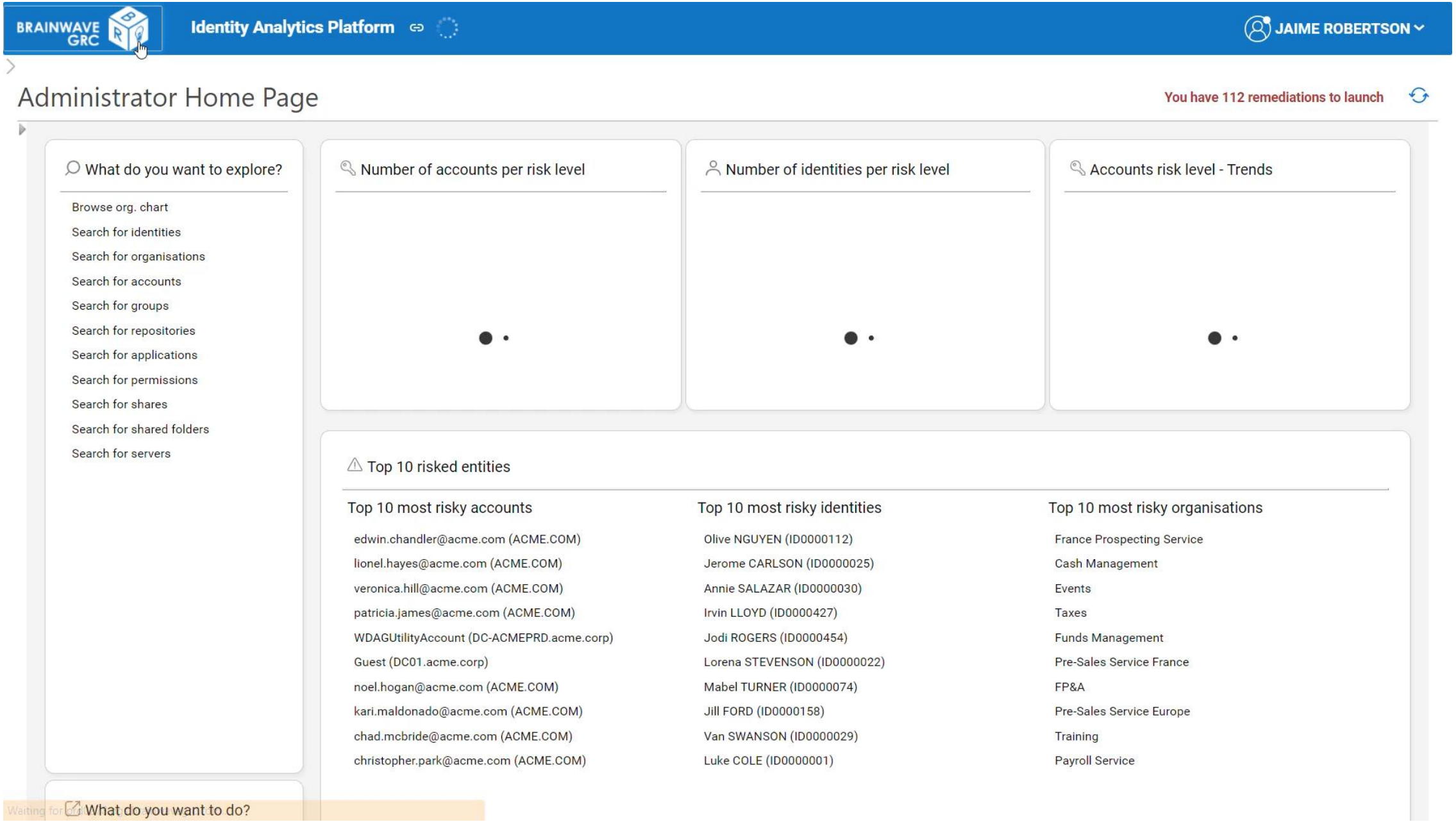
Accounts risk level - Trends



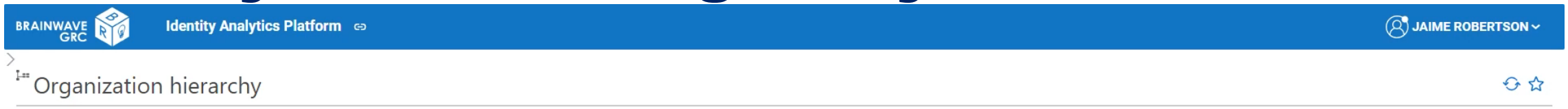
Top 10 risked entities

Top 10 most risky accounts	Top 10 most risky identities	Top 10 most risky organisations
edwin.chandler@acme.com (ACME.COM)	Olive NGUYEN (ID0000112)	France Prospecting Service
lionel.hayes@acme.com (ACME.COM)	Jerome CARLSON (ID0000025)	Cash Management
veronica.hill@acme.com (ACME.COM)	Annie SALAZAR (ID0000030)	Events
patricia.james@acme.com (ACME.COM)	Irvin LLOYD (ID0000427)	Taxes
WDAGUtilityAccount (DC-ACMEPRD.acme.corp)	Jodi ROGERS (ID0000454)	Funds Management
Guest (DC01.acme.corp)	Lorena STEVENSON (ID0000022)	Pre-Sales Service France
noel.hogan@acme.com (ACME.COM)	Mabel TURNER (ID0000074)	FP&A
kari.maldonado@acme.com (ACME.COM)	Jill FORD (ID0000158)	Pre-Sales Service Europe
chad.mcbride@acme.com (ACME.COM)	Van SWANSON (ID0000029)	Training
christopher.park@acme.com (ACME.COM)	Luke COLE (ID0000001)	Payroll Service

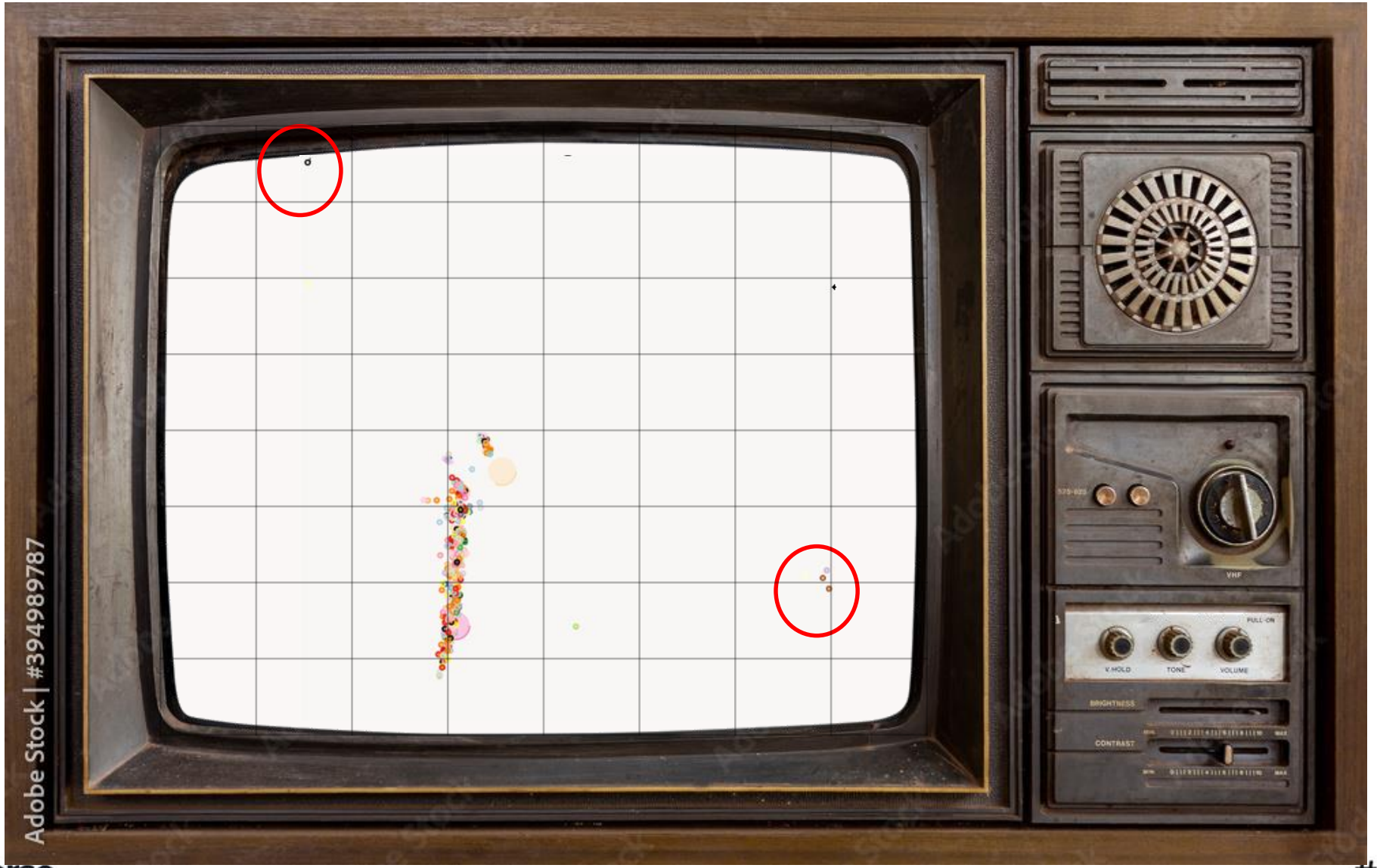
IT Checks: Accounts & Groups



Analysis: Clustering Analytics

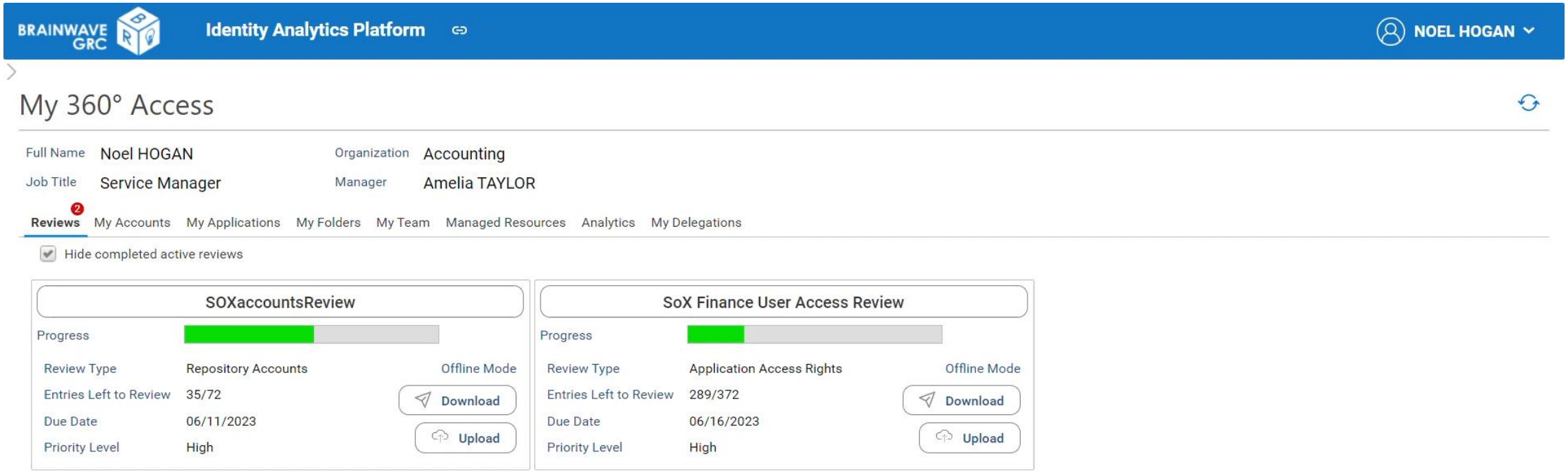


Analysis: Peer Groups

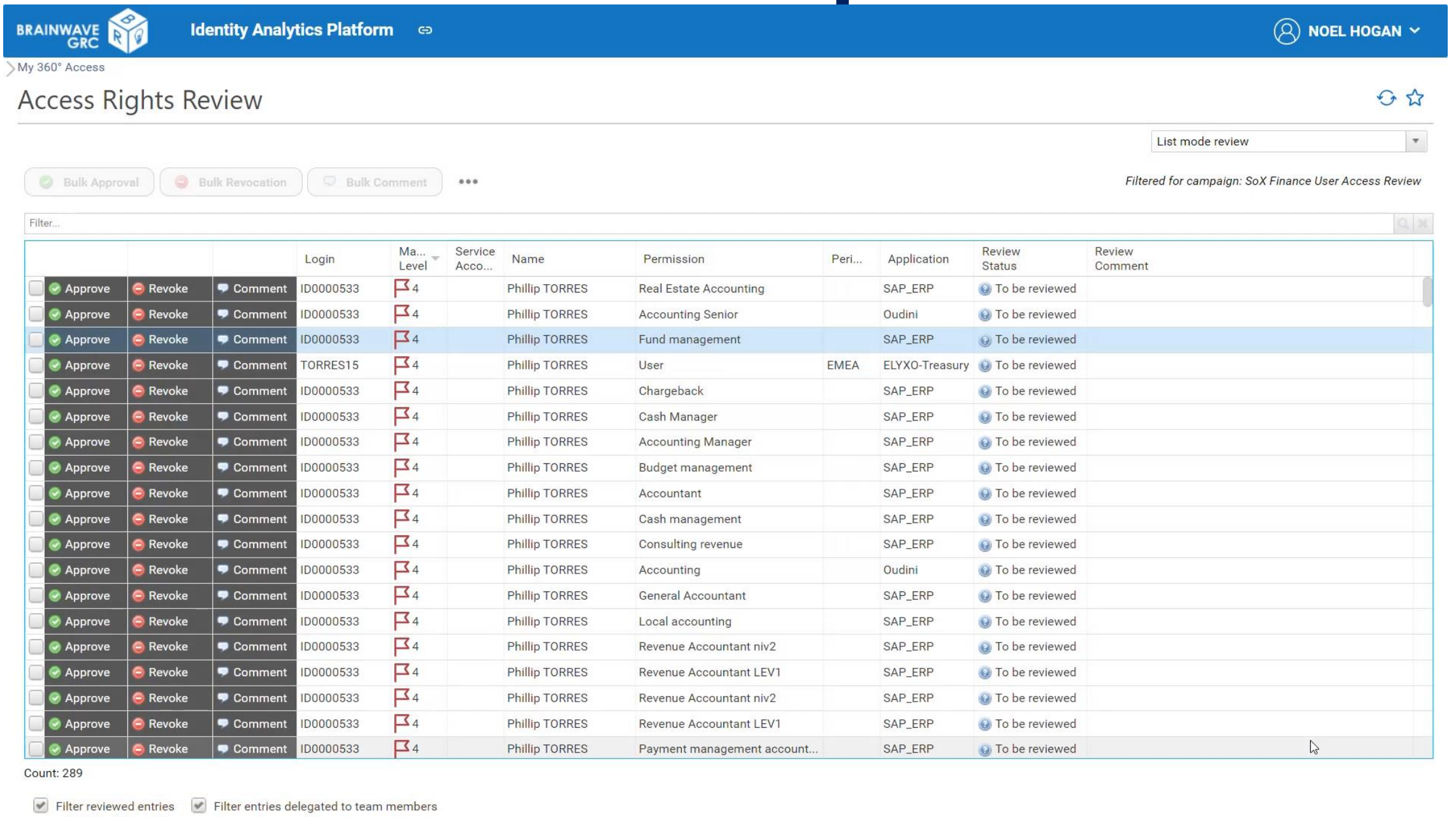


How to Make Business People ❤ Access Reviews

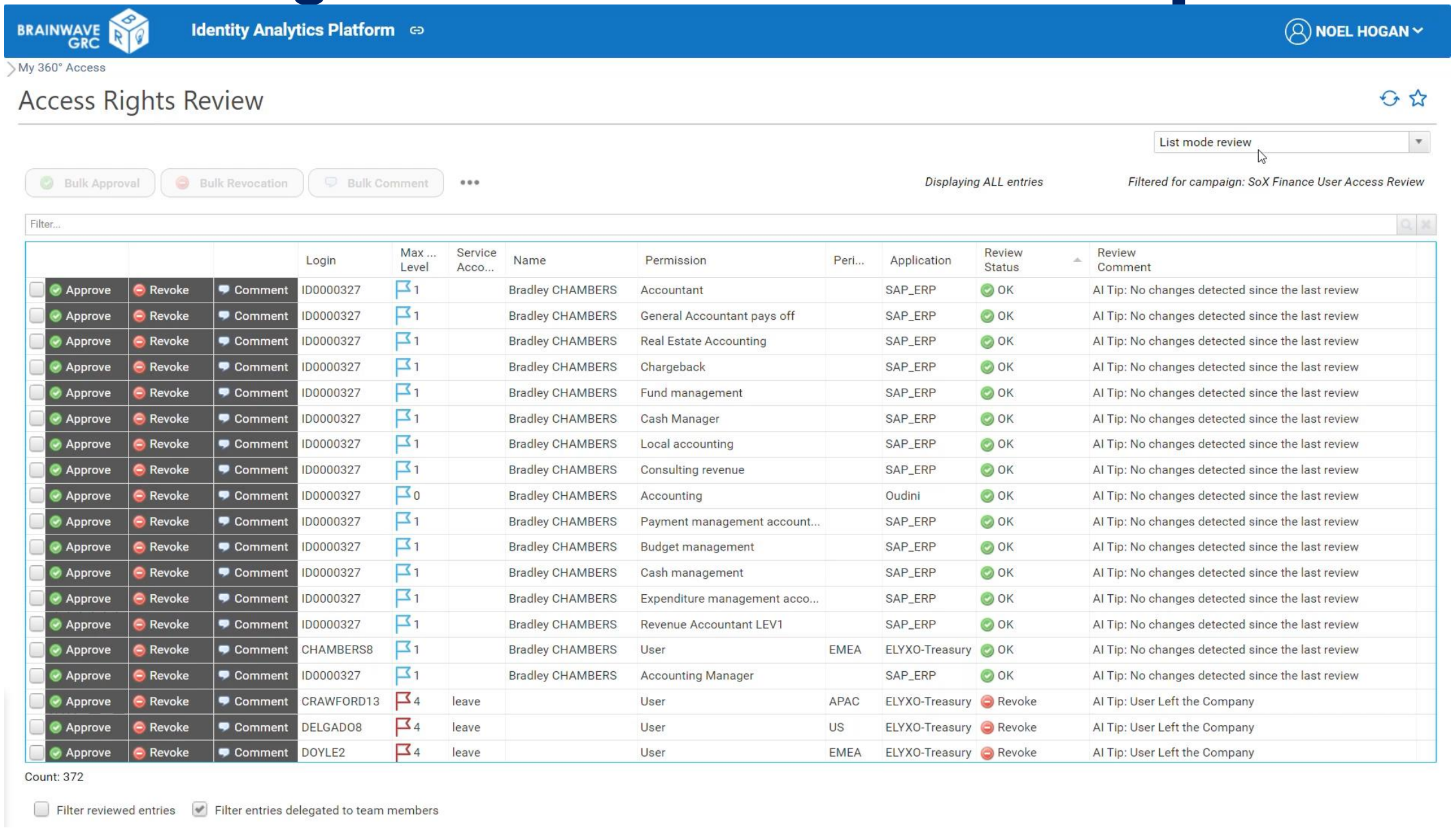
Provide Meaningful Context Information



Provide “Co-decision” Capabilities



Leverage Data Visualization Techniques

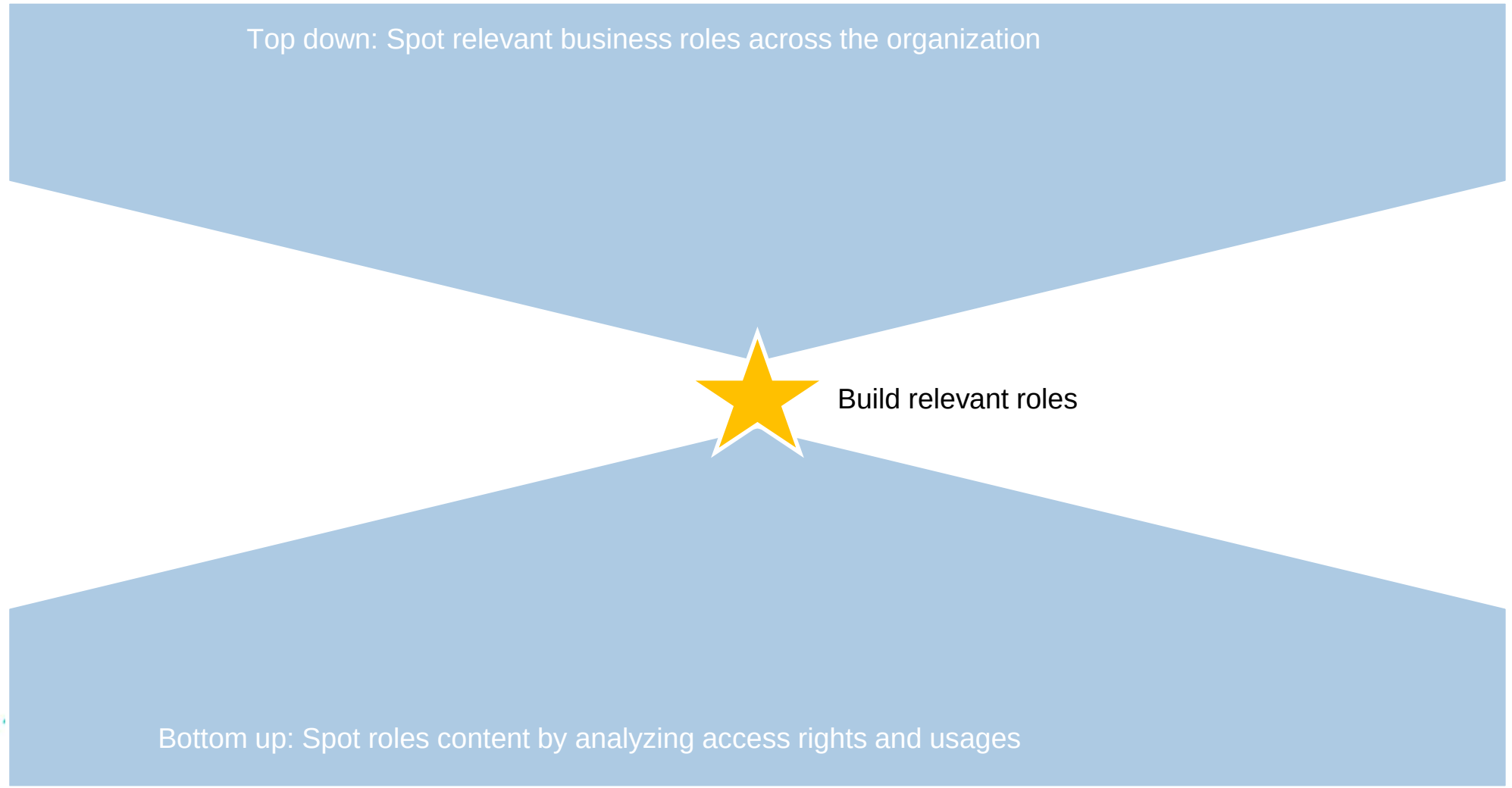


Introduce A Methodology For Role Mining, Involving Business People From Day One

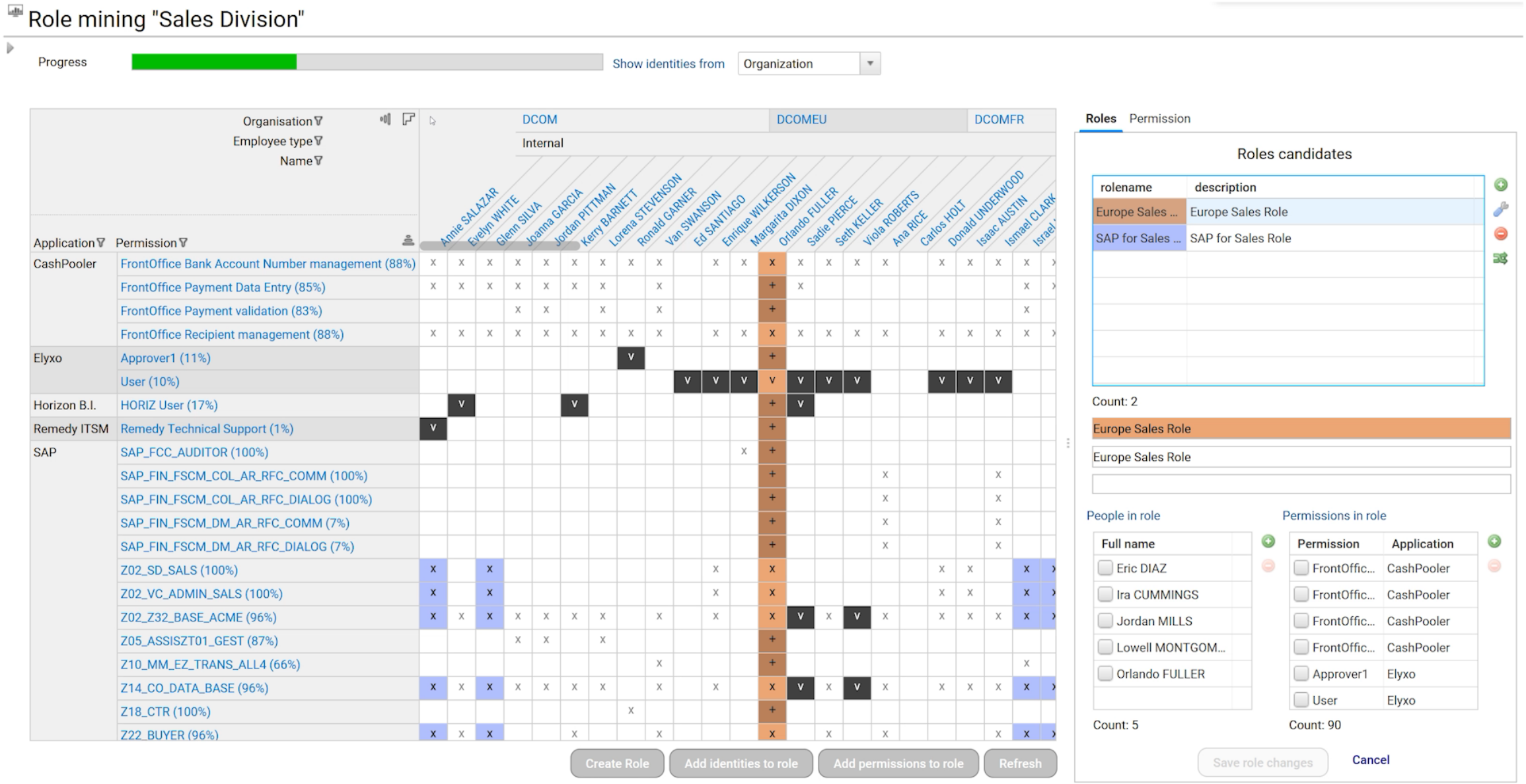
“A role is like a puppy, once you have one you need to care for it”

Common Pitfall: Launch a cryptic algorithms to design roles automatically without involving businessPeople

Role Mining Approach



Role Mining Experience

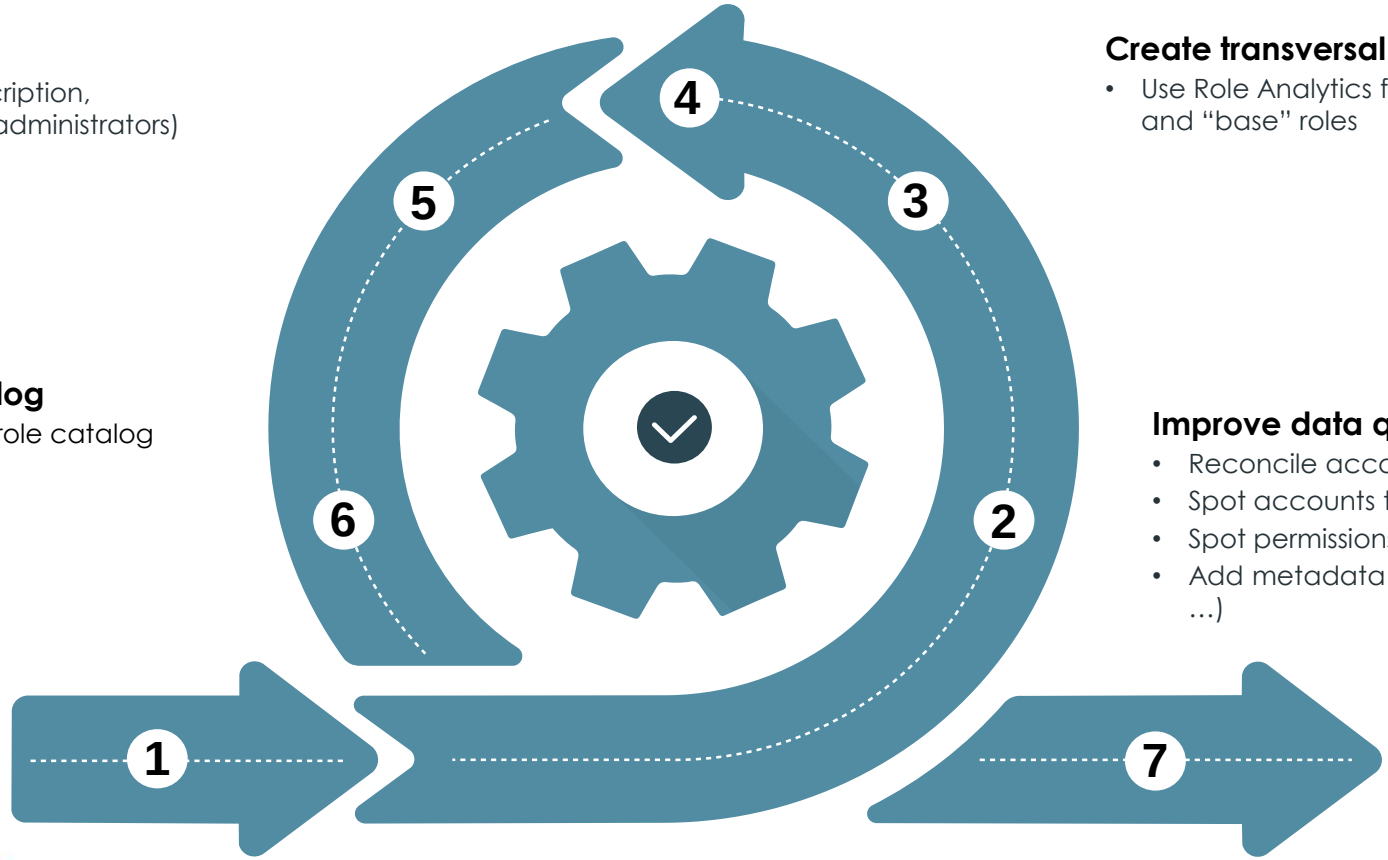


Role Mining Methodology

Role mining campaign and Role catalog creation
- Workshop based role mining campaign per sub-organization
- Use Role Mining feature to create role catalog

Document Roles
- Add information (description, sensitivity, approvers, administrators) per role, if needed

Create transversal roles
- Use Role Analytics features to design “transversal” and “base” roles



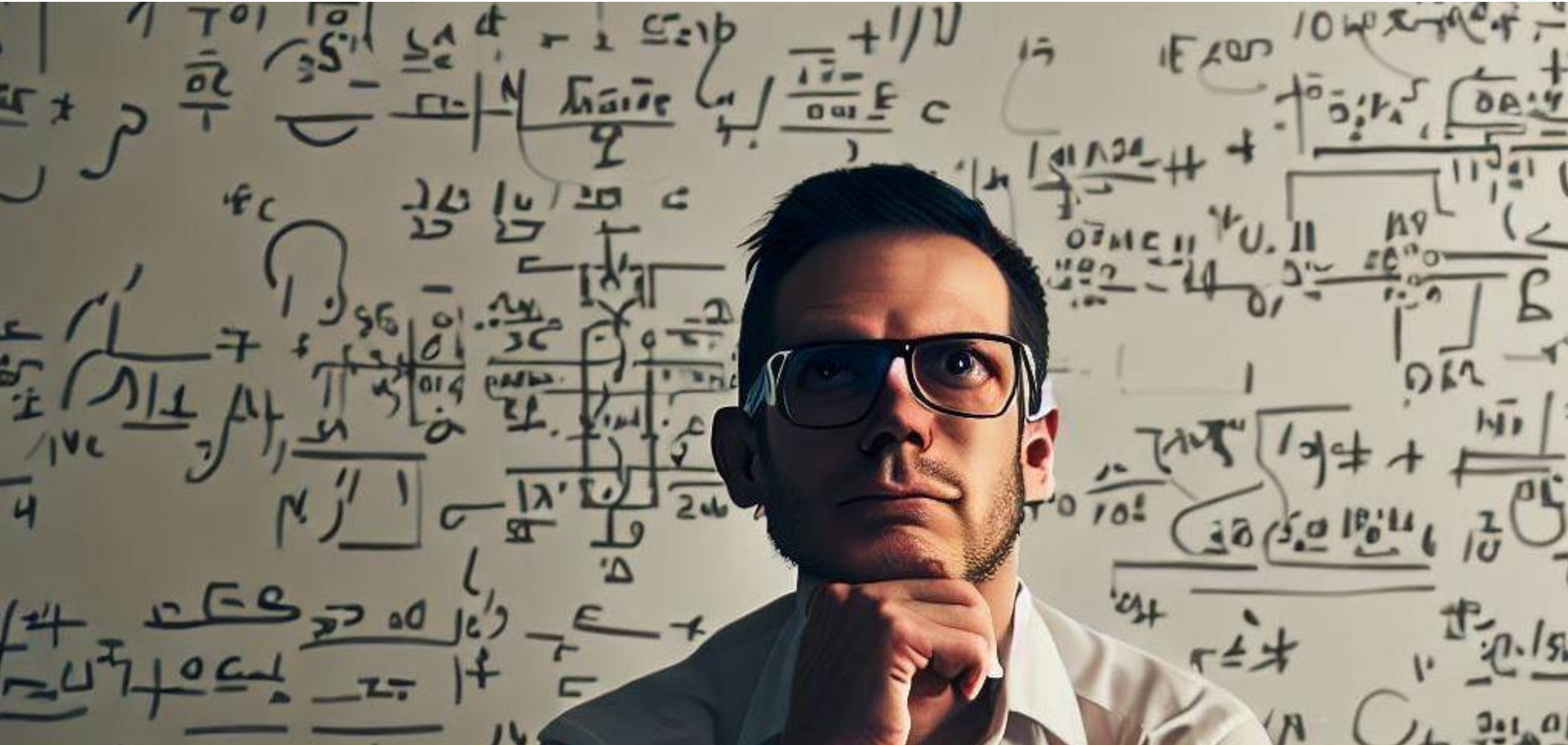
Validate the role catalog
- Create and review the role catalog

Improve data quality
- Reconcile accounts
- Spot accounts to disable
- Spot permissions to ignore
- Add metadata (permission description, sensitivity, …)

Build entitlement catalog
- Extract data and correlate it

Publish role catalog
- Generate role files

How to Compute Effective Risk Scoring



John Doe has admin access to a critical database instance….

…is it a risk?

It depends!

It **is not** a risk if he is the technical database owner

…It's just that its sensitive

It **is** a risk if:

- He is a simple business user
- Used to have access in a previous position
- …or left the company 3 months ago

How To Compute Effective Risk Scores To Focus On What's Really Important

- Common Pitfall:
  - Confusion between risky and sensitive configurations

ISO 27005 defines risk as "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

Effective Risk Scoring at a Glance

$$RiskScore_{rl} = f_{risklevel}(\Sigma(ControlDefects * resourcesSensitivityLevel))$$

$$RiskScore_{entity} = \Sigma(RiskScore_{rl})$$

Effective Risk Scoring Leverages Data Science

Entity	Risk Level	Control
JDOE75	1	Unused account
JDOE75	2	Password never expires
JDOE75	2	Password is too old
JDOE75	2	Atypical day/time for login
JDOE75	4	John left the company

32 bits unsigned integer risk score

RiskScore = 1*2^(8*0) + 3*2^(8*1) + 1*2^(8*3)

RiskScore = 16777985

Is 16777985 a relevant risk score for a business user?

Common Pitfall: Presenting « risk scores » to business users

Use Ranking and Max Risk Level instead!

HR Code	Firstname	Lastname	Risk Rank	Max Risk Level	Nb of risks
ID0000263	Manuel	BENNETT	→ 1	4	↗ 31
ID0000523	Kenneth	OSBORNE	→ 2	4	↗ 33
ID0000124	Dolores	GLOVER	↘ 3	4	↗ 31
ID0000321	Damon	WEBB	↗ 4	4	↗ 31
ID0000533	Phillip	TORRES	→ 5	4	↗ 40
ID0000388	Gladys	BERRY	↘ 6	4	↗ 31
ID0000844	Amanda	SHARP	↘ 7	4	↗ 24
ID0000632	Kerry	WADE	↘ 8	4	↗ 30
ID0000960	Jeanette	ADAMS	9	4	20
ID0000980	Jeannette	ANDERSON	9	4	30
ID0000963	Brett	TORRES	9	4	20
ID0000536	Toni	WILLIAMSON	↘ 9	4	↗ 21
ID0000144	Christine	MORGAN	↘ 9	4	↗ 26
ID0000082	Ana	RICE	↗ 10	4	→ 19
ID0000436	Jeanne	COBB	↘ 11	4	↗ 18
ID0000253	Walter	WATTS	↘ 12	4	↗ 17
ID0000013	Carlos	HOLT	↗ 13	4	→ 22
ID0000202	Priscilla	GORDON	↘ 14	4	↗ 19
ID0000678	Janie	NEWTON	↘ 14	4	↗ 30

Take Aways

Take Aways

1. **Quantity does not equal quality**
   - Do not just aggregate—correlate!
   - Move from a data posture to identity information
   - Introduce an Identity Data Fabric

2. **Empower the first line of defense: Business Users**
   - With an exception-based approach in your UIs
   - With actionable context information
   - With meaningful risk information
   - Leverage Identity Analytics

THANK YOU!

RADIANT LOGIC™

BRAINWAVE GRC
A Radiant Logic Company

BOOTH #1403