

# Getting Better Sleep With Analytics-Driven Identity Data Management



# Sebastien FAIVRE

CTO



# 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

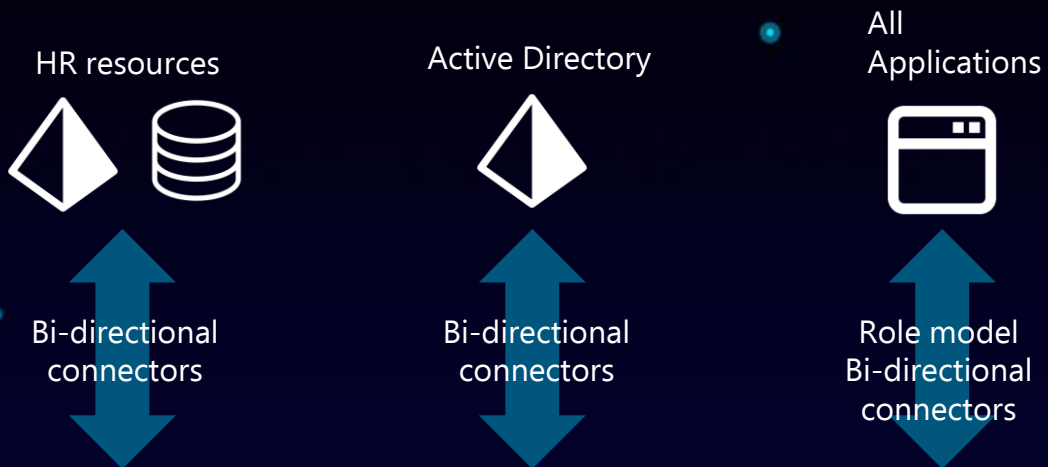
**210:** average number of days a hacker is present in the computer systems before attacking

**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



## 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



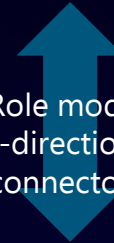
Bi-directional  
connectors



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

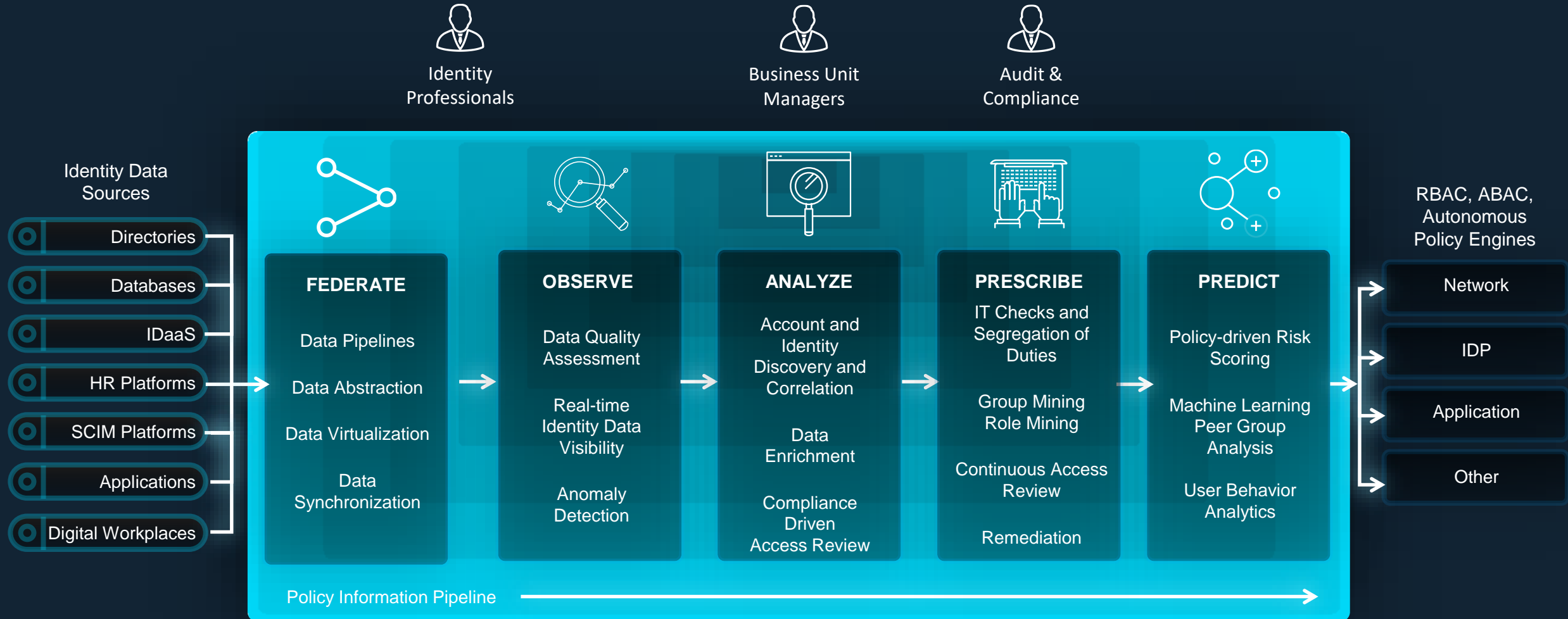


**Identity is everywhere:**

**How to tame the Identity problem?**



# A Proven Framework for Identity-First Security



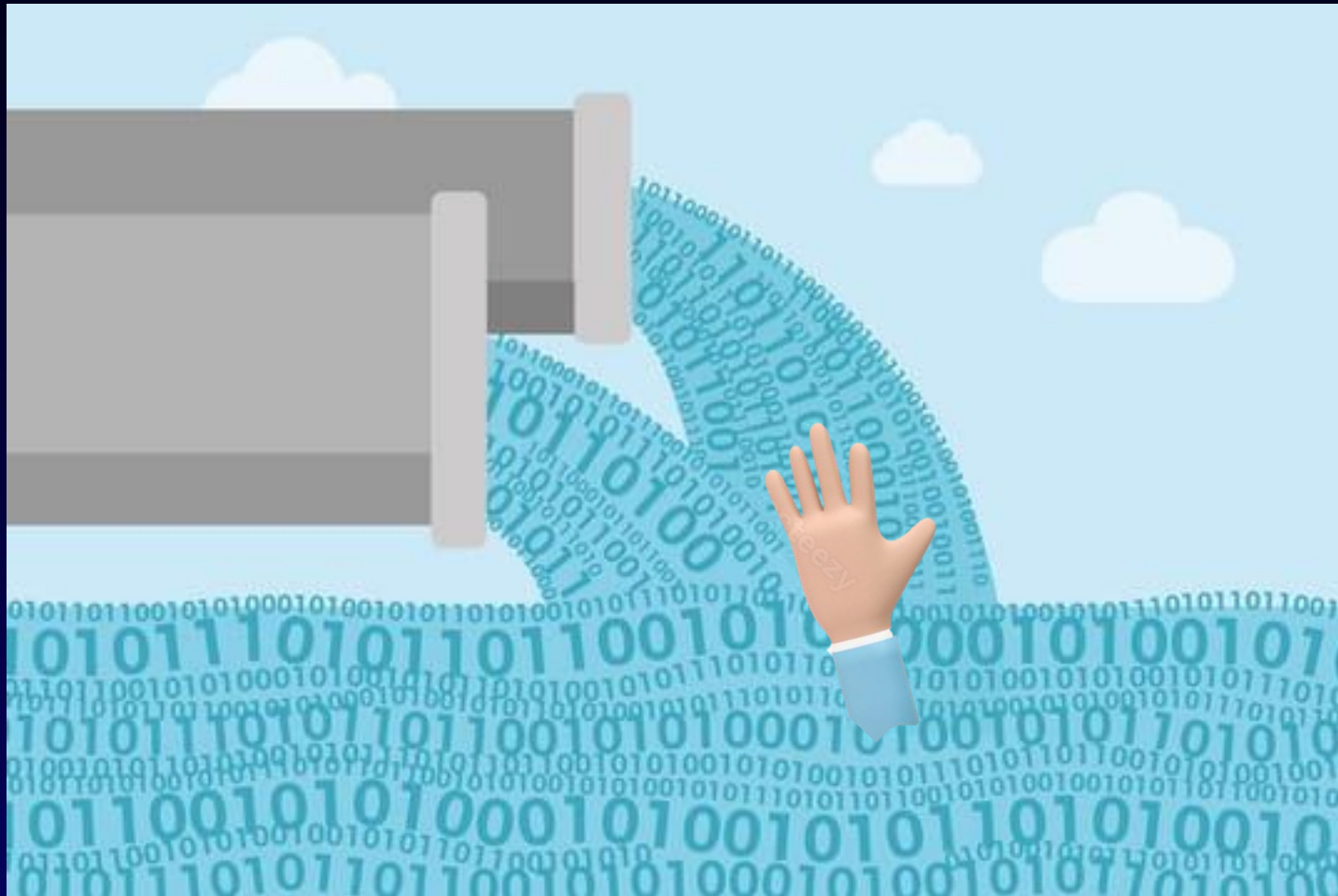
# Common pitfalls and misconceptions



# 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

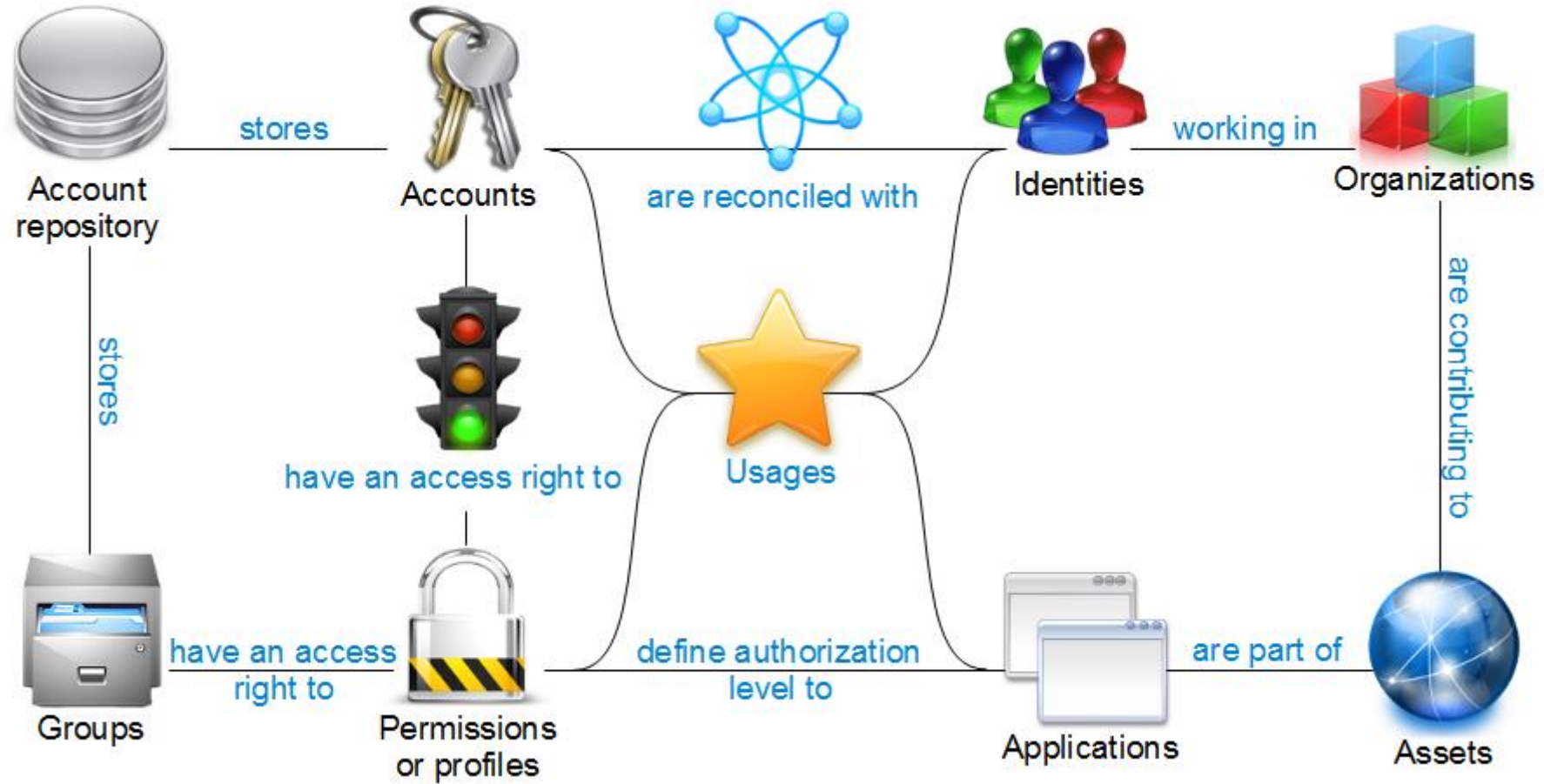


**Aggregation Alone is Not Enough!**

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





# 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



Identity Analytics Platform

JAIME ROBERTSON

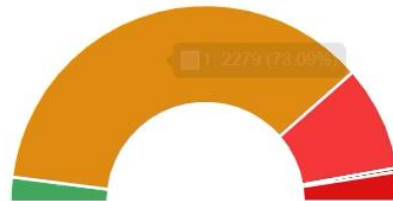
## Administrator Home Page

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

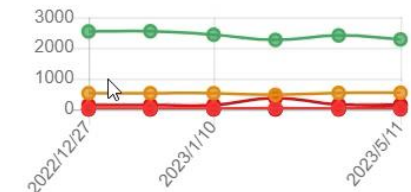
Number of accounts per risk level



Number of identities per risk level



Accounts risk level - Trends



Top 10 risked entities

### Top 10 most risky accounts

edwin.chandler@acme.com (ACME.COM)  
lionel.hayes@acme.com (ACME.COM)  
veronica.hill@acme.com (ACME.COM)  
patricia.james@acme.com (ACME.COM)  
WDAGUtilityAccount (DC-ACMEPRD.acme.corp)  
Guest (DC01.acme.corp)  
noel.hogan@acme.com (ACME.COM)  
kari.maldonado@acme.com (ACME.COM)  
chad.mcbride@acme.com (ACME.COM)  
christopher.park@acme.com (ACME.COM)

### Top 10 most risky identities

Olive NGUYEN (ID0000112)  
Jerome CARLSON (ID0000025)  
Annie SALAZAR (ID0000030)  
Irvin LLOYD (ID0000427)  
Jodi ROGERS (ID0000454)  
Lorena STEVENSON (ID0000022)  
Mabel TURNER (ID0000074)  
Jill FORD (ID0000158)  
Van SWANSON (ID0000029)  
Luke COLE (ID0000001)

### Top 10 most risky organisations

France Prospecting Service  
Cash Management  
Events  
Taxes  
Funds Management  
Pre-Sales Service France  
FP&A  
Pre-Sales Service Europe  
Training  
Payroll Service

What do you want to do?

# IT Checks: Identities

## 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

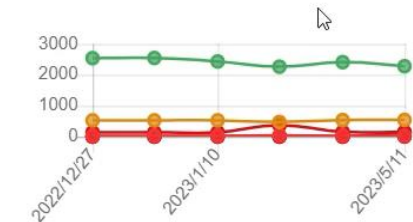
Number of accounts per risk level



Number of identities per risk level



Accounts risk level - Trends



### Top 10 risked entities

#### Top 10 most risky accounts

edwin.chandler@acme.com (ACME.COM)  
lionel.hayes@acme.com (ACME.COM)  
veronica.hill@acme.com (ACME.COM)  
patricia.james@acme.com (ACME.COM)  
WDAGUtilityAccount (DC-ACMEPRD.acme.corp)  
Guest (DC01.acme.corp)  
noel.hogan@acme.com (ACME.COM)  
kari.maldonado@acme.com (ACME.COM)  
chad.mcbride@acme.com (ACME.COM)  
christopher.park@acme.com (ACME.COM)

#### Top 10 most risky identities

Olive NGUYEN (ID0000112)  
Jerome CARLSON (ID0000025)  
Annie SALAZAR (ID0000030)  
Irvin LLOYD (ID0000427)  
Jodi ROGERS (ID0000454)  
Lorena STEVENSON (ID0000022)  
Mabel TURNER (ID0000074)  
Jill FORD (ID0000158)  
Van SWANSON (ID0000029)  
Luke COLE (ID0000001)

#### Top 10 most risky organisations

France Prospecting Service  
Cash Management  
Events  
Taxes  
Funds Management  
Pre-Sales Service France  
FP&A  
Pre-Sales Service Europe  
Training  
Payroll Service

What do you want to do?

# IT Checks: Accounts & Groups



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

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

edwin.chandler@acme.com (ACME.COM)  
lionel.hayes@acme.com (ACME.COM)  
veronica.hill@acme.com (ACME.COM)  
patricia.james@acme.com (ACME.COM)  
WDAGUtilityAccount (DC-ACMEPRD.acme.corp)  
Guest (DC01.acme.corp)  
noel.hogan@acme.com (ACME.COM)  
kari.maldonado@acme.com (ACME.COM)  
chad.mcbride@acme.com (ACME.COM)  
christopher.park@acme.com (ACME.COM)

#### Top 10 most risky identities

Olive NGUYEN (ID0000112)  
Jerome CARLSON (ID0000025)  
Annie SALAZAR (ID0000030)  
Irvin LLOYD (ID0000427)  
Jodi ROGERS (ID0000454)  
Lorena STEVENSON (ID0000022)  
Mabel TURNER (ID0000074)  
Jill FORD (ID0000158)  
Van SWANSON (ID0000029)  
Luke COLE (ID0000001)

#### Top 10 most risky organisations

France Prospecting Service  
Cash Management  
Events  
Taxes  
Funds Management  
Pre-Sales Service France  
FP&A  
Pre-Sales Service Europe  
Training  
Payroll Service

# Analysis: Clustering Analytics



Identity Analytics Platform

JAIME ROBERTSON

>  
I= Organization hierarchy





# Analysis: Peer Groups



Adobe Stock | #394989787

# How to Make Business People ❤️👍 Access Reviews

# Provide Meaningful Context Information



Identity Analytics Platform

NOEL HOGAN

## My 360° Access

Full Name Noel HOGAN

Organization Accounting

Job Title Service Manager

Manager Amelia TAYLOR

Reviews

My Accounts My Applications My Folders My Team Managed Resources Analytics My Delegations

☒ Hide completed active reviews

### SOXaccountsReview

Progress



Review Type Repository Accounts

Offline Mode

Entries Left to Review 35/72

Download

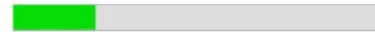
Due Date 06/11/2023

Priority Level High

Upload

### SoX Finance User Access Review

Progress



Review Type Application Access Rights

Offline Mode

Entries Left to Review 289/372

Download

Due Date 06/16/2023

Priority Level High

Upload

# Provide “Co-decision” Capabilities



Identity Analytics Platform

NOEL HOGAN

My 360° Access

## Access Rights Review



List mode review

Bulk Approval Bulk Revocation Bulk Comment

Filtered for campaign: SoX Finance User Access Review

Filter...											
			Login	Ma... Level	Service Acco...	Name	Permission	Peri...	Application	Review Status	Review Comment
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Real Estate Accounting		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Accounting Senior		Oudini	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Fund management		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	TORRES15	P4	Phillip TORRES	User	EMEA	ELYXO-Treasury	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Chargeback		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Cash Manager		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Accounting Manager		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Budget management		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Accountant		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Cash management		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Consulting revenue		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Accounting		Oudini	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	General Accountant		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Local accounting		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Revenue Accountant niv2		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Revenue Accountant LEV1		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Revenue Accountant niv2		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Revenue Accountant LEV1		SAP_ERP	To be reviewed	
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000533	P4	Phillip TORRES	Payment management account...		SAP_ERP	To be reviewed	

Count: 289

☒ Filter reviewed entries ☒ Filter entries delegated to team members



# Leverage Data Visualization Techniques



Identity Analytics Platform

NOEL HOGAN

My 360° Access

## Access Rights Review



List mode review

Bulk Approval Bulk Revocation Bulk Comment

Displaying ALL entries

Filtered for campaign: SoX Finance User Access Review

Filter...

			Login	Max ... Level	Service Acco...	Name	Permission	Peri...	Application	Review Status	Review Comment
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Accountant		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	General Accountant pays off		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Real Estate Accounting		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Chargeback		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Fund management		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Cash Manager		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Local accounting		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Consulting revenue		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	0	Bradley CHAMBERS	Accounting		Oudini	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Payment management account...		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Budget management		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Cash management		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Expenditure management acco...		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Revenue Accountant LEV1		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	CHAMBERS8	1	Bradley CHAMBERS	User	EMEA	ELYXO-Treasury	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	ID0000327	1	Bradley CHAMBERS	Accounting Manager		SAP_ERP	OK	AI Tip: No changes detected since the last review
<input type="checkbox"/>	Approve	Revoke	Comment	CRAWFORD13	4		User	APAC	ELYXO-Treasury	Revoke	AI Tip: User Left the Company
<input type="checkbox"/>	Approve	Revoke	Comment	DELGADO8	4		User	US	ELYXO-Treasury	Revoke	AI Tip: User Left the Company
<input type="checkbox"/>	Approve	Revoke	Comment	DOYLE2	4		User	EMEA	ELYXO-Treasury	Revoke	AI Tip: User Left the Company

Count: 372

☐ Filter reviewed entries ☒ Filter entries delegated to team members

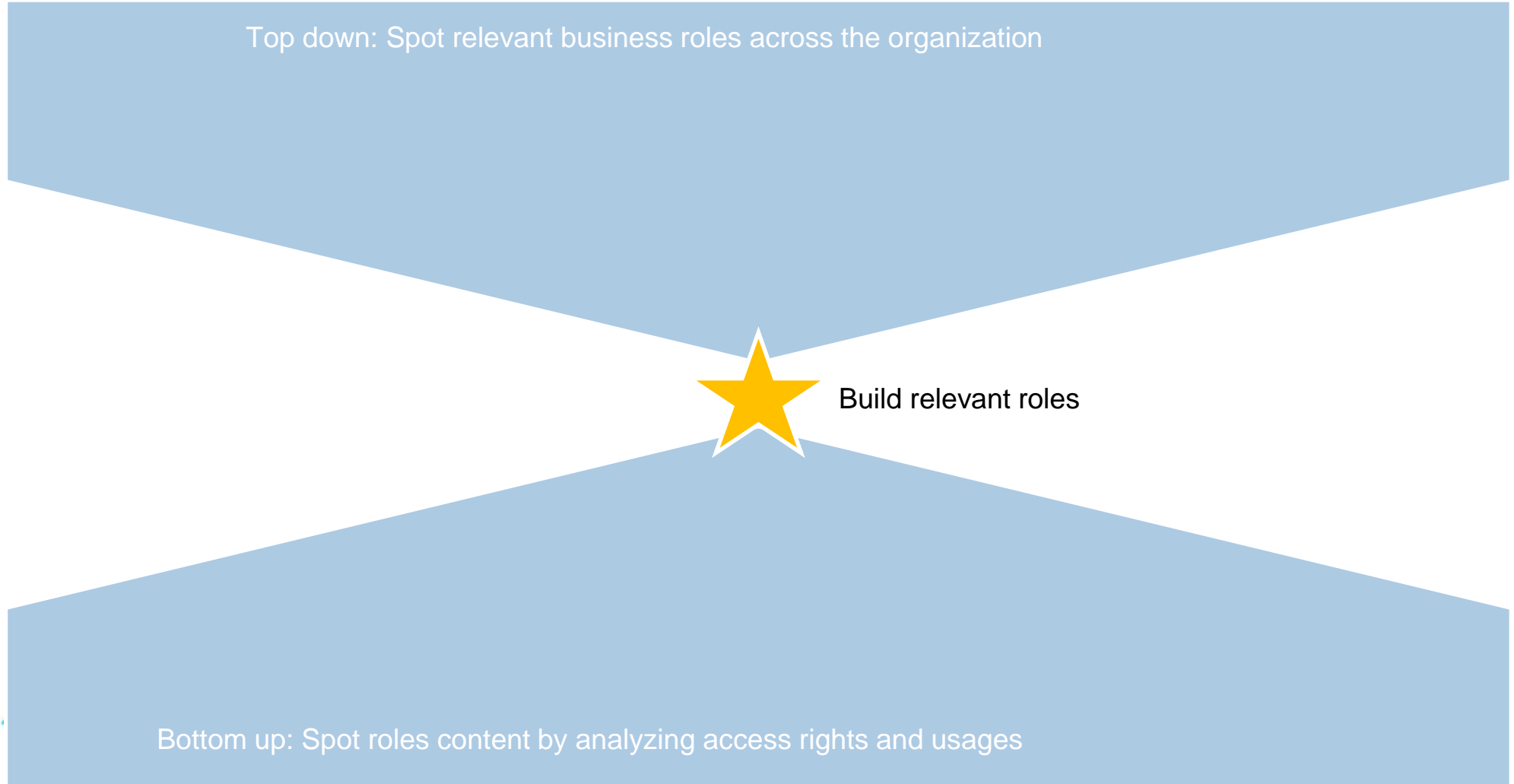


# Introduce A Methodology For Role Mining, Involving Business People From Day One

*“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 "Sales Division"

Progress

Show identities from

Organization

		DCOM										DCOMEU					DCOMFR				
Organisation ▾		Internal																			
Employee type ▾																					
Name ▾																					

Create Role

Add identities to role

Add permissions to role

Refresh

Roles Permission

### Roles candidates

rolename	description
Europe Sales ...	Europe Sales Role
SAP for Sales ...	SAP for Sales Role

Count: 2

Europe Sales Role

Europe Sales Role

People in role

Full name
<input type="checkbox"/> Eric DIAZ
<input type="checkbox"/> Ira CUMMINGS
<input type="checkbox"/> Jordan MILLS
<input type="checkbox"/> Lowell MONTGOM...
<input type="checkbox"/> Orlando FULLER

Count: 5

Permissions in role

Permission	Application
<input type="checkbox"/> FrontOffic...	CashPooler
<input type="checkbox"/> FrontOffic...	CashPooler
<input type="checkbox"/> FrontOffic...	CashPooler
<input type="checkbox"/> FrontOffic...	CashPooler
<input type="checkbox"/> Approver1	Elyxo
<input type="checkbox"/> User	Elyxo

Count: 90

Save role changes

Cancel

# 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

### Validate the role catalog

- Create and review the role catalog

### Build entitlement catalog

- Extract data and correlate it

### Create transversal roles

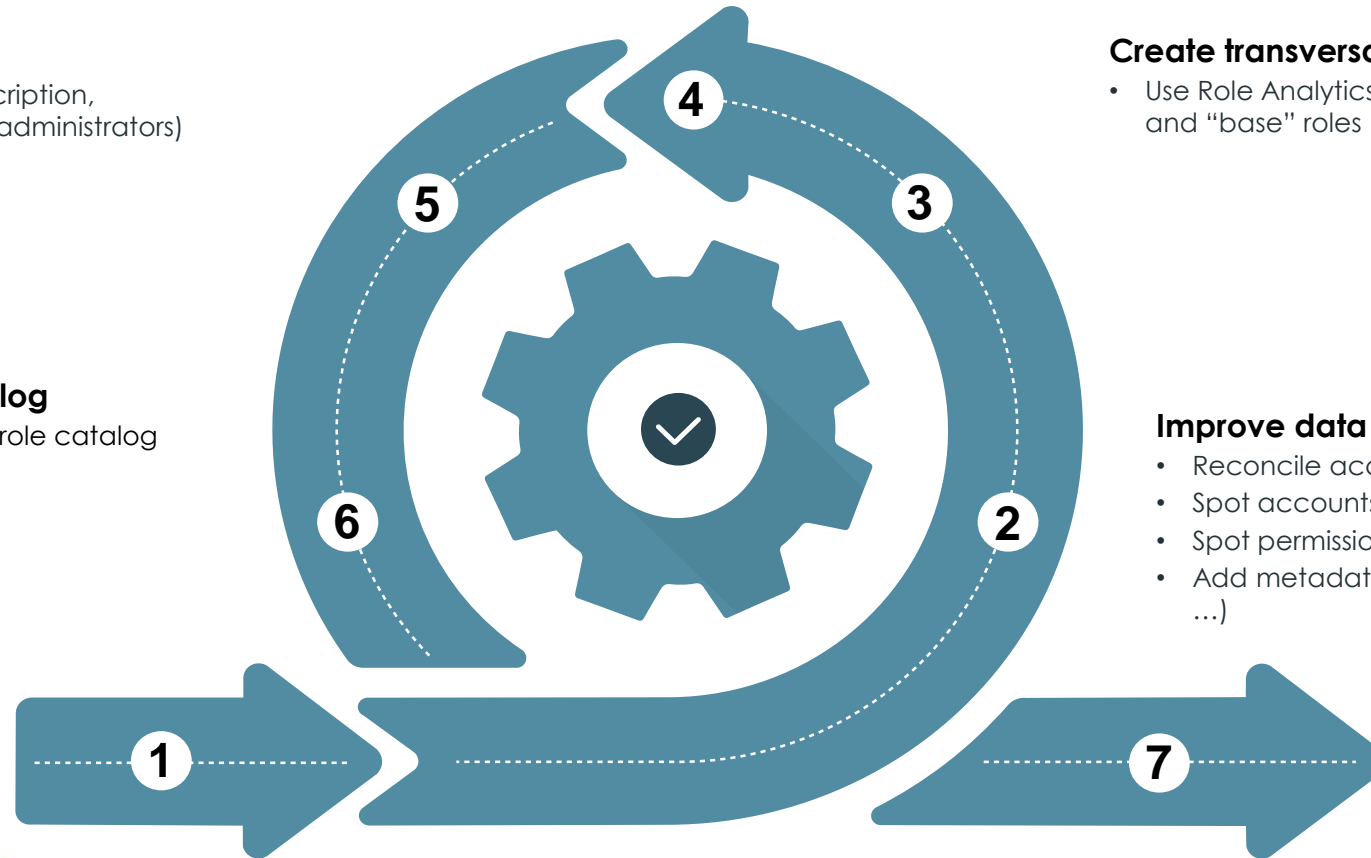
- Use Role Analytics features to design “transversal” and “base” roles

### Improve data quality

- Reconcile accounts
- Spot accounts to disable
- Spot permissions to ignore
- Add metadata (permission description, sensitivity, ...)

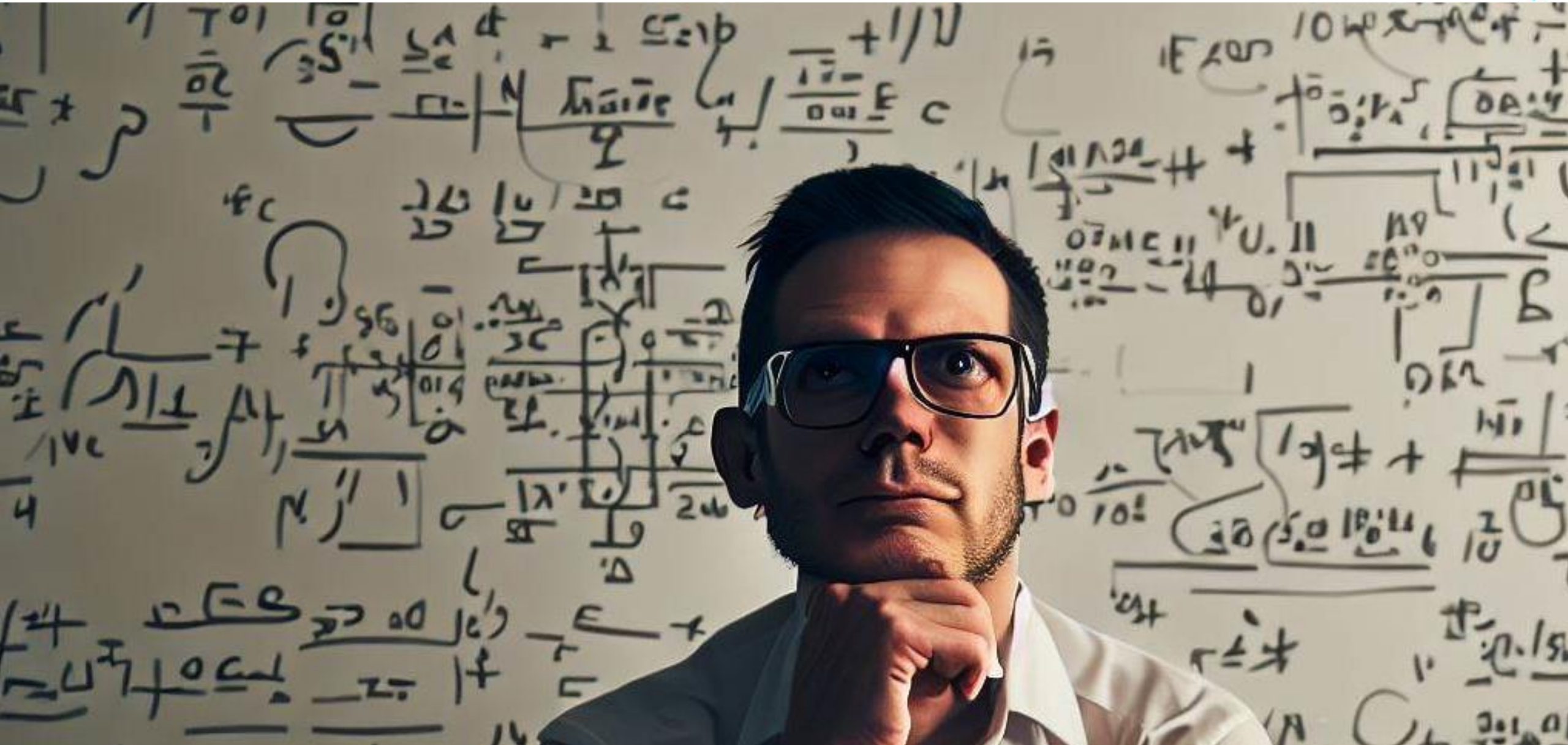
### Publish role catalog

- 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

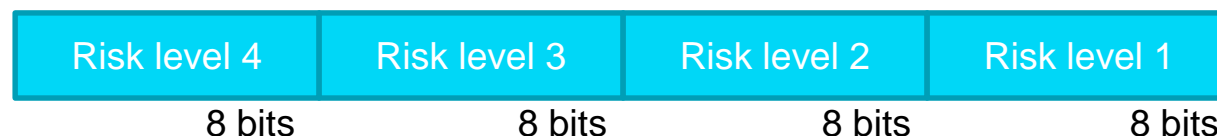
$$\text{RiskScore}_{rl} = f_{\text{risklevel}}(\Sigma(\text{ControlDefects} * \text{resourcesSensitivityLevel}))$$

$$\text{RiskScore}_{\text{entity}} = \Sigma(\text{RiskScore}_{rl})$$

# 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



$$\text{RiskScore} = 1 * 2^{(8*0)} + 3 * 2^{(8*1)} + 1 * 2^{(8*3)}$$

$$\text{RiskScore} = 16777985$$

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	Lanie	NEWTON	↘ 14	⚠ 4	↗ 20

# 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!



**BRAINWAVE**  
**GRC**  
A Radiant Logic Company



**BOOTH #1403**



**#identiverse**