MidPoint Community Meetup 2025

Role Mining in MidPoint Workshop

Ing. Tadeáš Chrapovič

Java developer at Evolveum

Evolveum

Workshop Agenda

- Presentation Part
    - Overview of role mining concepts and approach
- Practical Part - Overview
    - Hands-on exploration of role mining tools and features
- Coffee Break ☺
    - 30 minutes to recharge and reflect
- Practical Part - Scenarios
    - Work through different role mining scenarios
- Conclusion
    - Key takeaways and applications of role mining
- Discussion and Questions
    - Open floor for question and insights

Presentation

Agenda

- Understanding Role Mining
  - What is role mining?
  - Why is it important?
- Key Benefits of Role Mining
  - Simplifies access management
  - Reduce administrative work
- The Role Mining Process and Technology
  - Data gathering
  - Discovering role suggestions
- Migrating to Business Roles
  - Transitioning from chaos to structure

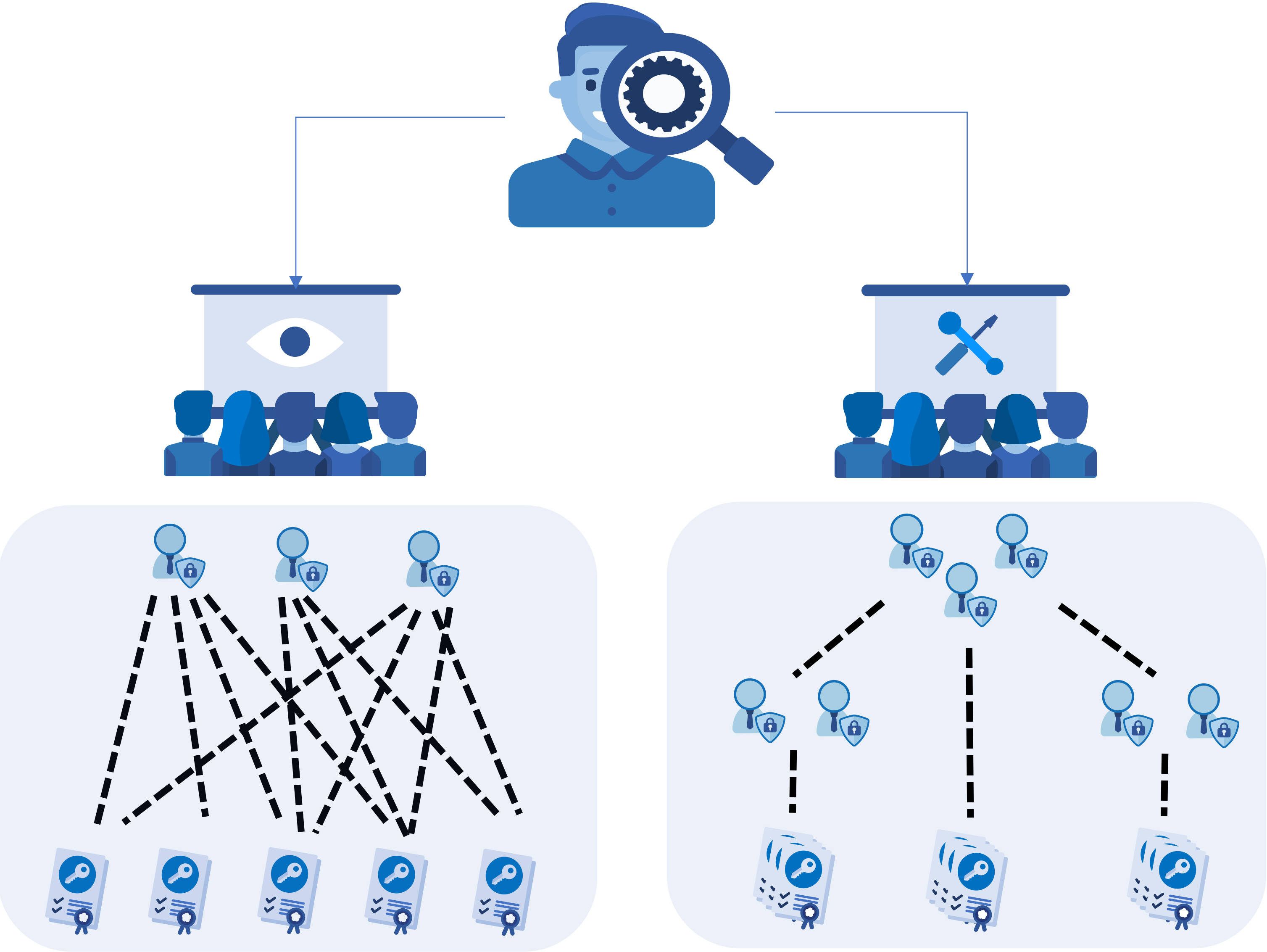
Bottom-Up RBAC Approach

Data-Driven Approach
Focuses on analysing existing user-permission relationship

Cluster-Based Discovery
Groups user that act similar from access rights perspective

Uncover hidden information
Identifies hidden roles that manual processes may miss

Refinement
Discovered roles need to be refined and validated



The Essence of Role Mining

Analysis-Driven Process

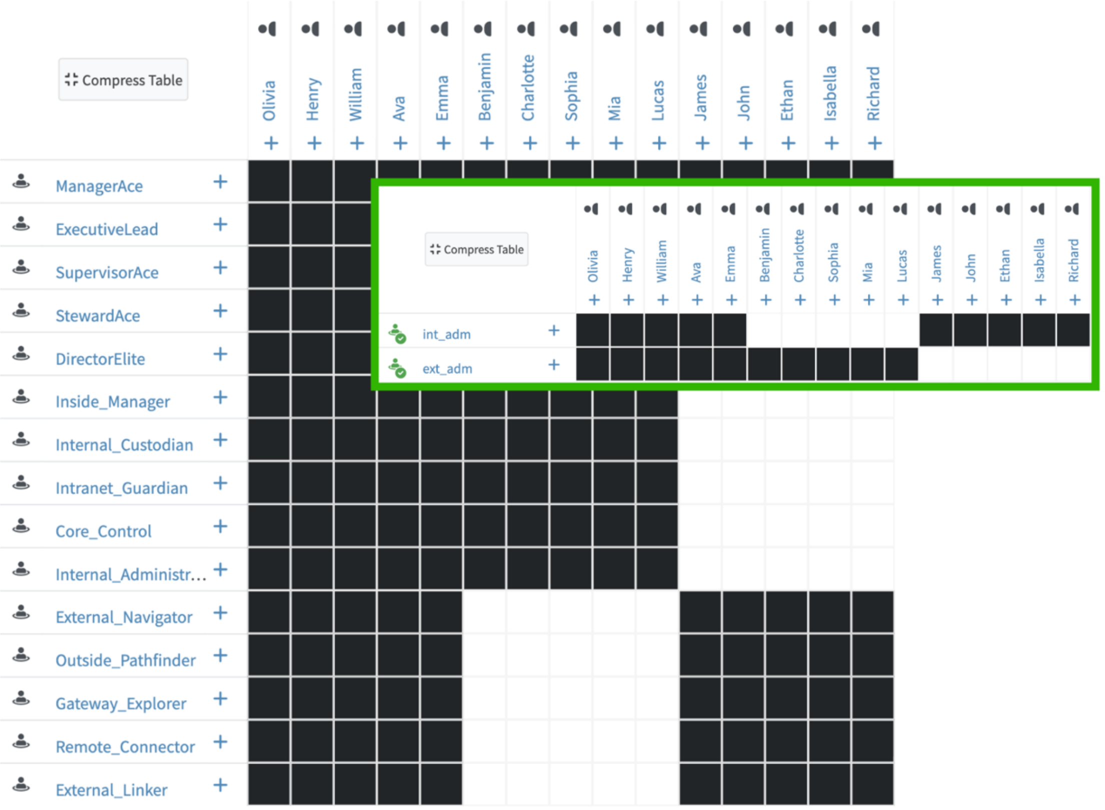
- Utilizing Data-Driven Insights for Role Definition
- Uncovering Patterns and Clusters in User Permissions

Simplification

- Reducing Complexity for Access Management
- Aligning Permissions with Clear Business Roles

Algorithmic Data Processing

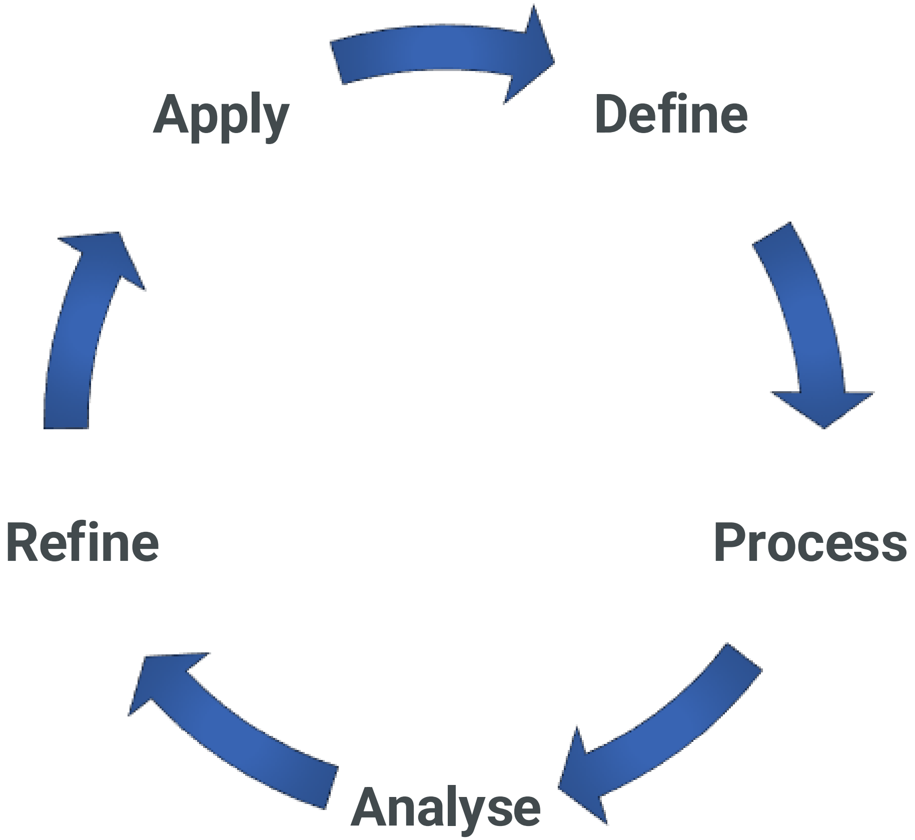
- Leveraging Advanced Algorithms and ML Techniques
- Processing Access Control Data for Hidden Insights



	Olivia	Henry	William	Ava	Emma	Benjamin	Charlotte	Sophia	Mia	Lucas	James	John	Ethan	Isabella	Richard
ManagerAce	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
ExecutiveLead	■	■	■	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
SupervisorAce	■	■	■	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
StewardAce	■	■	■	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
DirectorElite	■	■	■	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Inside_Manager	■	■	■	■	■	■	■	■	■	■					
Internal_Custodian	■	■	■	■	■	■	■	■	■	■					
Intranet_Guardian	■	■	■	■	■	■	■	■	■	■					
Core_Control	■	■	■	■	■	■	■	■	■	■					
Internal_Administr...	■	■	■	■	■	■	■	■	■	■					
External_Navigator	■	■	■	■	■						■	■	■	■	■
Outside_Pathfinder	■	■	■	■	■						■	■	■	■	■
Gateway_Explorer	■	■	■	■	■						■	■	■	■	■
Remote_Connector	■	■	■	■	■						■	■	■	■	■
External_Linker	■	■	■	■	■						■	■	■	■	■

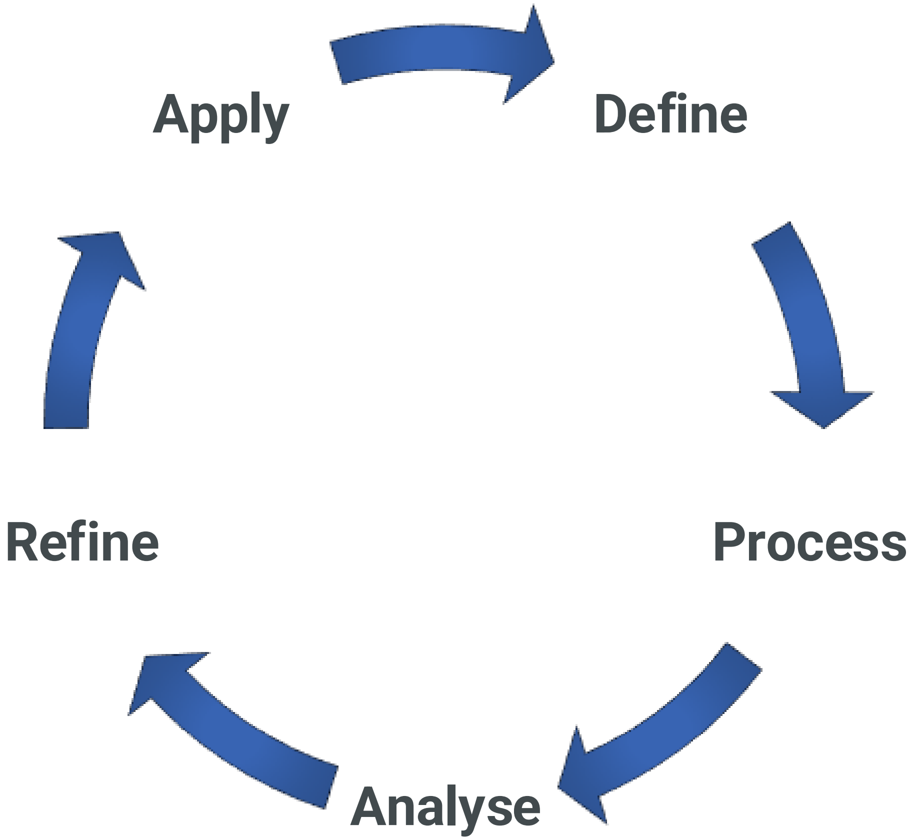
	Olivia	Henry	William	Ava	Emma	Benjamin	Charlotte	Sophia	Mia	Lucas	James	John	Ethan	Isabella	Richard
int_adm	■	■	■	■	■						■	■	■	■	■
ext_adm	■	■	■	■	■	■	■	■	■	■					

Process insights



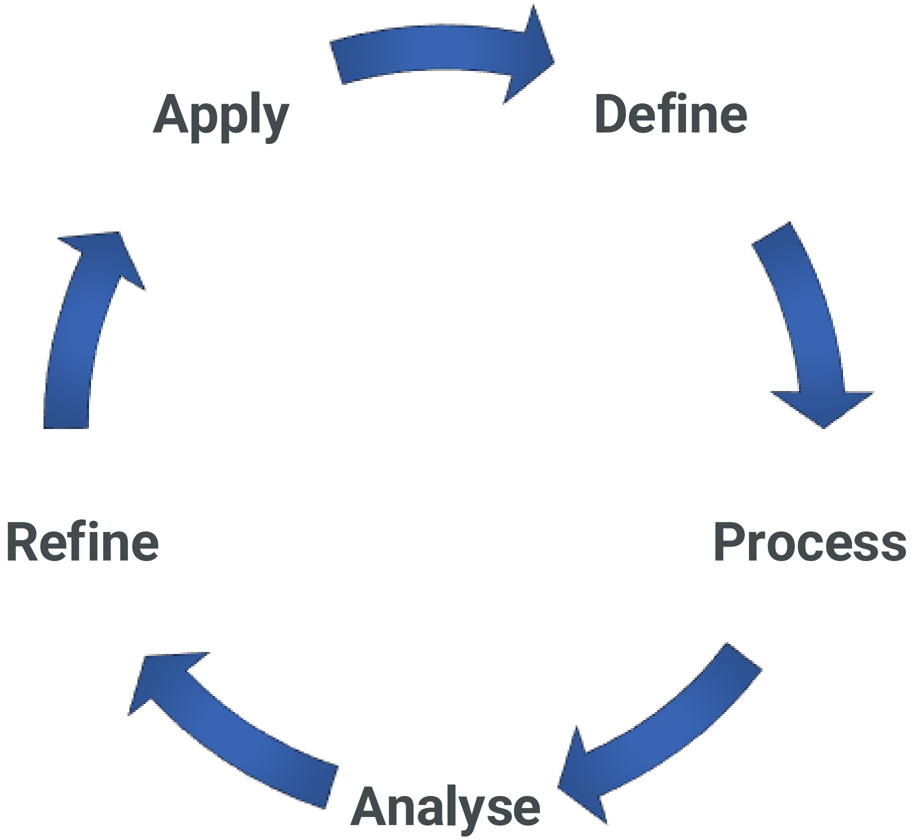
- Role Mining Initiation
  - Define aim to achieve
  - Specify data we should use
  - Analyse additional information

Process insights



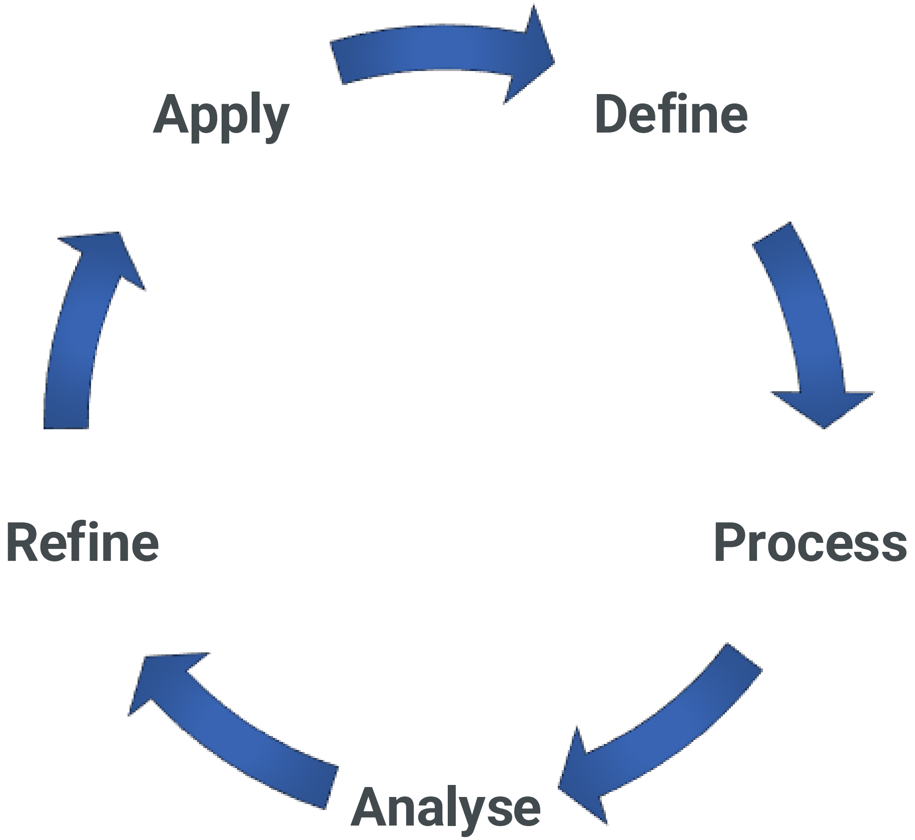
- Role Mining Initiation
- **Processing Operation**
  - **Identify similarities – Data Clustering**
  - **Detect possible reduction - Pattern Detection**

Process insights



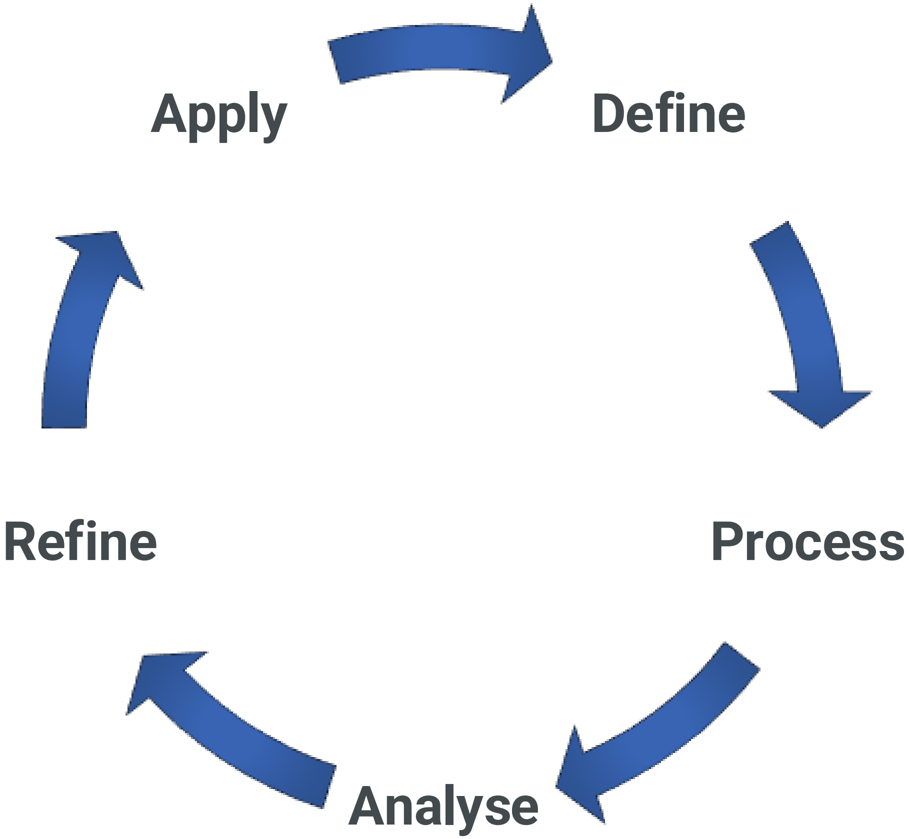
- Role Mining Initiation
- Processing Operation
- **Refinement of Business Role Candidates**
  - **Identify potential candidates**
  - **Role engineering process**

Process insights



- Role Mining Initiation
- Processing Operation
- Refinement of Business Role Candidates
- **Integration and Implementation**
  - **Migration process**
  - **Review result**

Process insights



- Role Mining Initiation
- Processing Operation
- Refinement of Business Role Candidates
- Integration and Implementation
- **Iteration and Continuous Improvement**
  - **Repeat cycle ☺**

Impact of Role Mining

- Challenges without Role Mining:
  - Complex access data navigation
  - Manual customization of permissions
- Role Mining Solution:
  - Pattern identification and proposed modifications
  - Smart alignment of access rights with roles
- Benefits:
  - Enhanced security and reduced manual effort
  - Empowerment for innovation and security reinforcement

Practical part

Overview

Setting Up the Environment

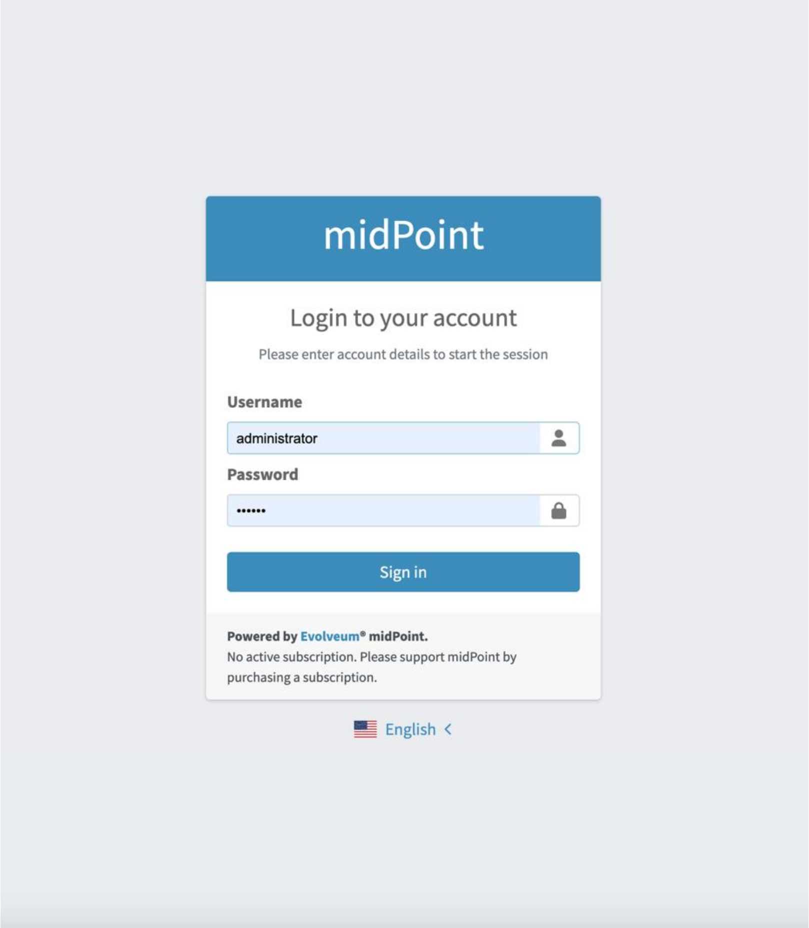
- Download source project
  - https://download.evolveum.com/workshops/mcm-2025/role-mining-env.zip
- Build server
  - **cd role-mining-env**
  - **docker compose up –d**
- Host
  - http://localhost:8080
  - Credential name: *Administrator*
  - Credential password: *Rol3Mmc25*
- Reset environment
  - **docker compose down -v**
  - **docker compose up –d**

What's practical part include

- Data Overview
  - Understand the structure and content of system data
  - Review existing user-role relations
- Role Mining Process Initiation
  - Explore role mining possibilities
  - Configure and execute role analysis
- Role Mining results Overview
  - Review role mining result
  - Learn how to collect and interpret information from the results
- Migration Process
  - Apply the refined role structure to improve system efficiency

Practical part - Data Overview

- Roles are assigned directly to users, instead of using business model interpretation
- Users and roles are categories based on their behavioural e.g. Location
- Roles have security classifications with is represent by “security tier” attribute (tier-1 to tier-5) reflecting access sensitivity
- Some roles may be outdated or is limited (from a member count perspective)



midPoint

Login to your account

Please enter account details to start the session

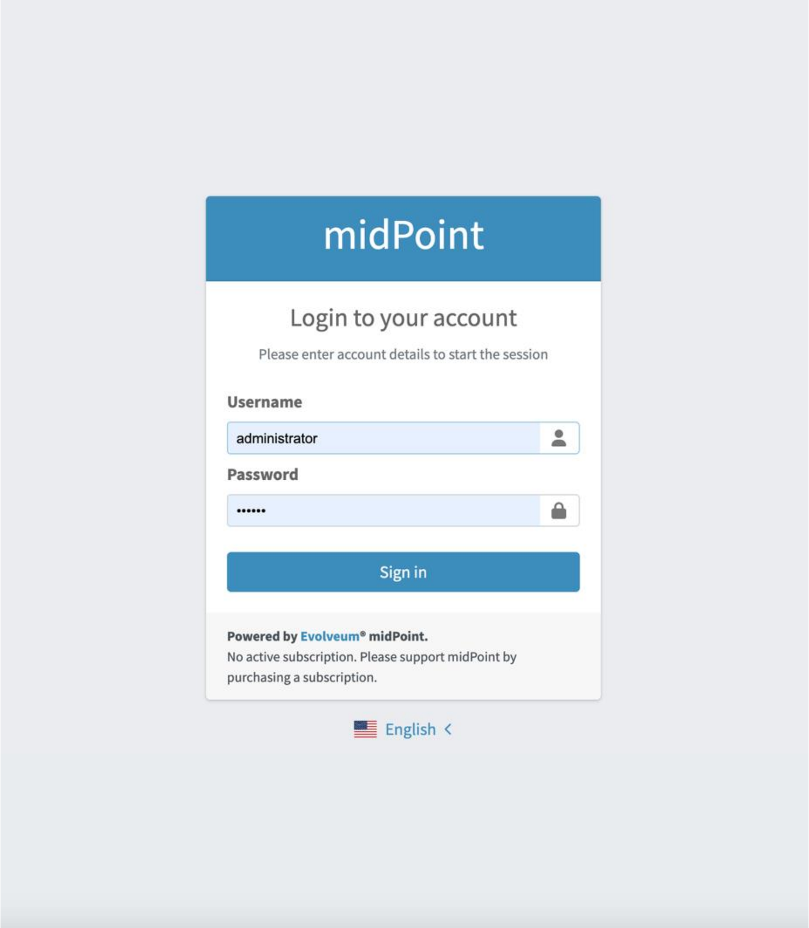
Username: administrator

Password: ••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Process Initiation

- Provides key insights into current role assignments for better access management
- Offers multiple predefined analysis modes tailored for specific scenarios
- Customizable process requiring minimal system knowledge, adaptable to various needs
- Acts as a snapshot with automatic updates possibility to keep analysis relevant over time



midPoint

Login to your account

Please enter account details to start the session

Username: administrator

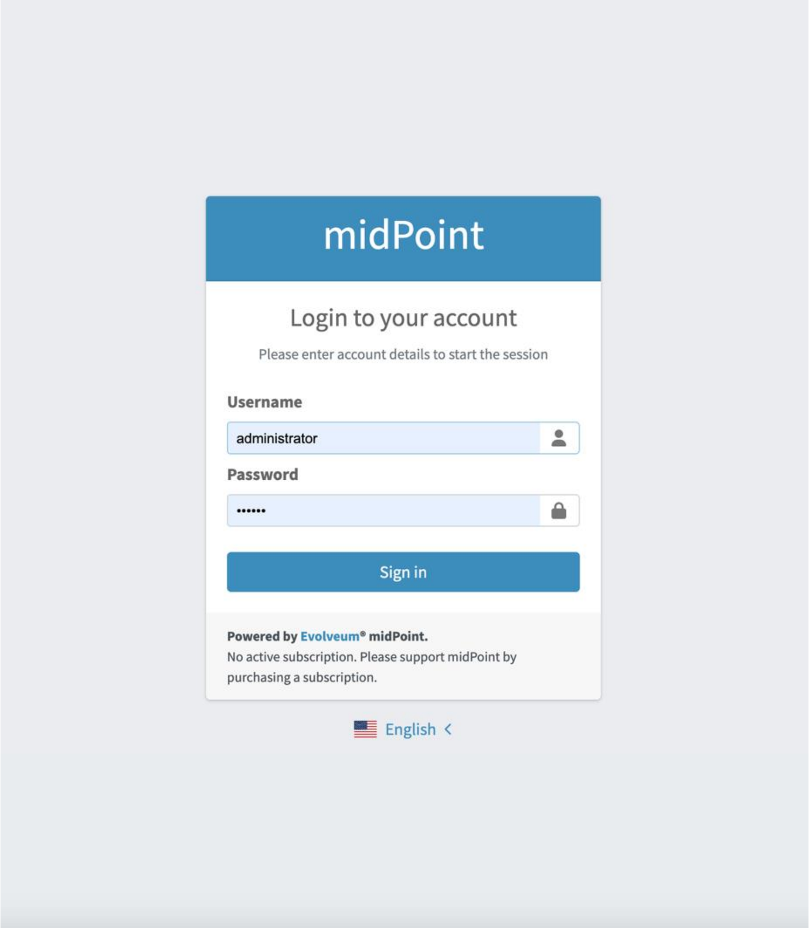
Password: ••••••

Powered by Evolveum® midPoint.

No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Results Overview

- Provide a detailed overview of processed objects including noise, for complete analysis
- Uncover hidden patterns in user-role assignments and analyse it from different perspectives
- Visualize user-role assignments through an interactive user-permission matrix
- Provide possibility to refine results by focusing on meaningful patterns



midPoint

Login to your account

Please enter account details to start the session

Username

administrator

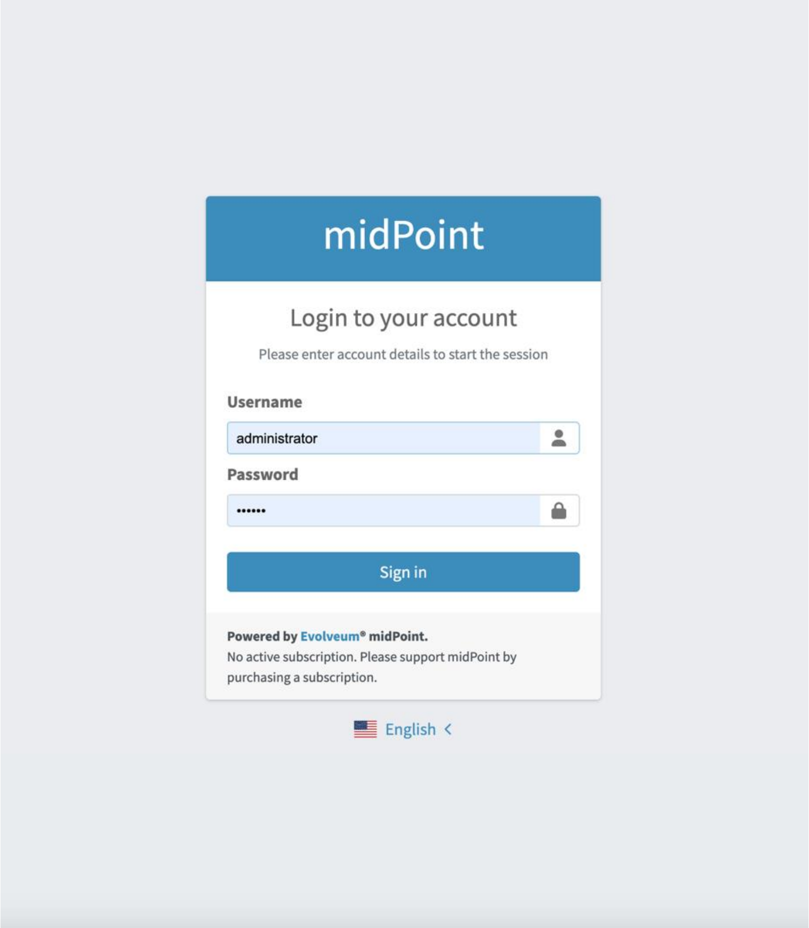
Password

••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Migration Process

- Role mining functionality helped us identify patterns in user access and suggested new roles
- The role mining component provides space for the entire role engineering process
- The migration process remove all duplicate assignments and activated the new business role
- The new created business role is ready to be assigned to new employees, simplifying access management



midPoint

Login to your account

Please enter account details to start the session

Username

administrator

Password

••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Reset the Environment

- Navigate to the Docker project:
  - **cd role-mining-env**
- Stop and remove containers, networks, and volumes:
  - **docker compose down -v**
- Recreate containers in detached mode:
  - **docker compose up -d**

☕☕ Coffee Break ☕☕

☺

Reset the Environment

- Navigate to the Docker project:
  - **cd role-mining-env**
- Stop and remove containers, networks, and volumes:
  - **docker compose down -v**
- Recreate containers in detached mode:
  - **docker compose up -d**

Practical part

Scenarios

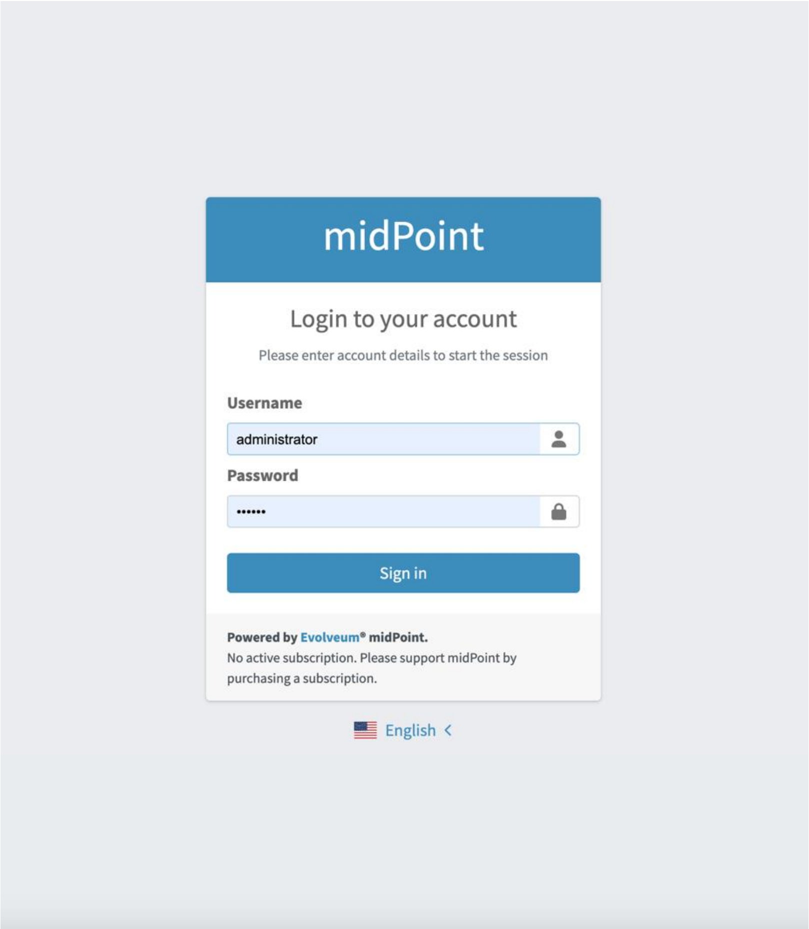
Practical part include

- Identify and define system Birthright Business Access
  - Discover Employee system common roles structures
  - Discover Contractor system common roles structures
- Identify and Define Location Business Access
  - Discover location related access structures
  - Ensure that user has their required access
- Identify and Define Department Business Access
  - Discover department related access structures
  - Support specific organisation
- Identify and Define Profession Business Access
  - Discover most common job-based access structures
  - Exclude unwanted objects

Practical part - Birthright Business Access

- **Scenario 1:** Discover Employee system common roles
  - Automatically assigned to 95% of users
  - Core functions like Active Directory group membership, email access.
  - Ensure users have basic access
- **Scenario 2:** Discover Contractor system common roles
  - Automatically assigned to 5% of users
  - Core functions
  - Ensure users have basic access

NOTE: Ensures contractors birthright role provide appropriate access without unnecessary privileges.



midPoint

Login to your account

Please enter account details to start the session

Username: administrator

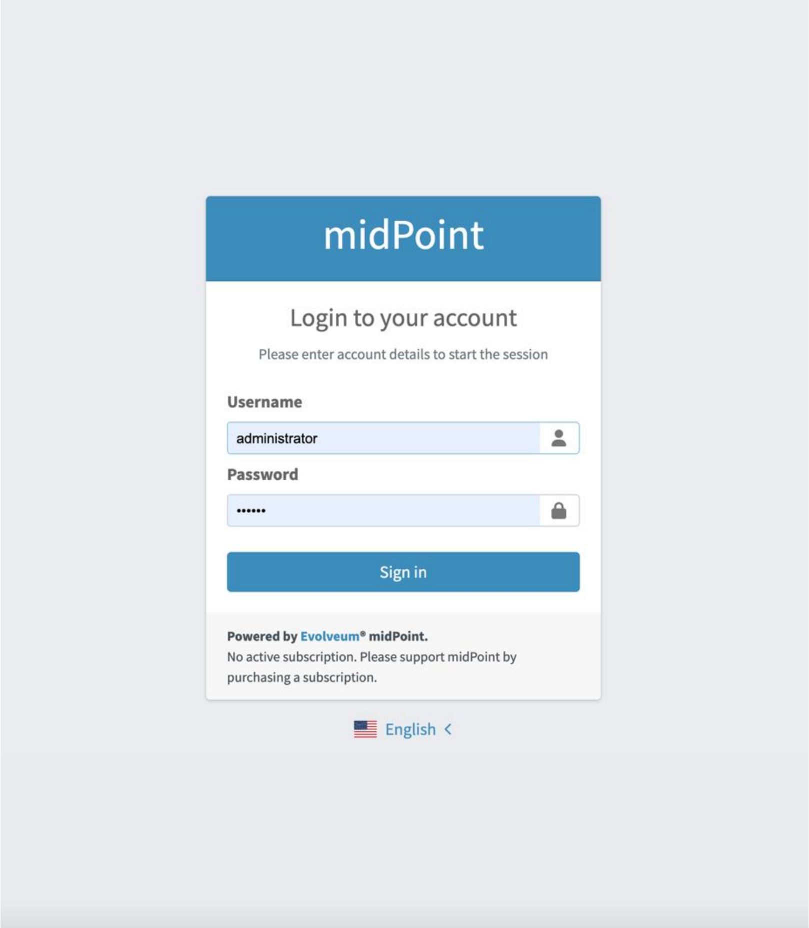
Password: ••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Location Business Access

- **Scenario:** Discover location roles
  - Assigned to unknown number of users
  - Work with location category roles
  - Ensure users have basic access

NOTE: Location roles are distributed as a pack. With means if user is from *Lisbon,* then he should have e.g. Lisbon AD & Lisbon Building Access.



midPoint

Login to your account

Please enter account details to start the session

Username: administrator

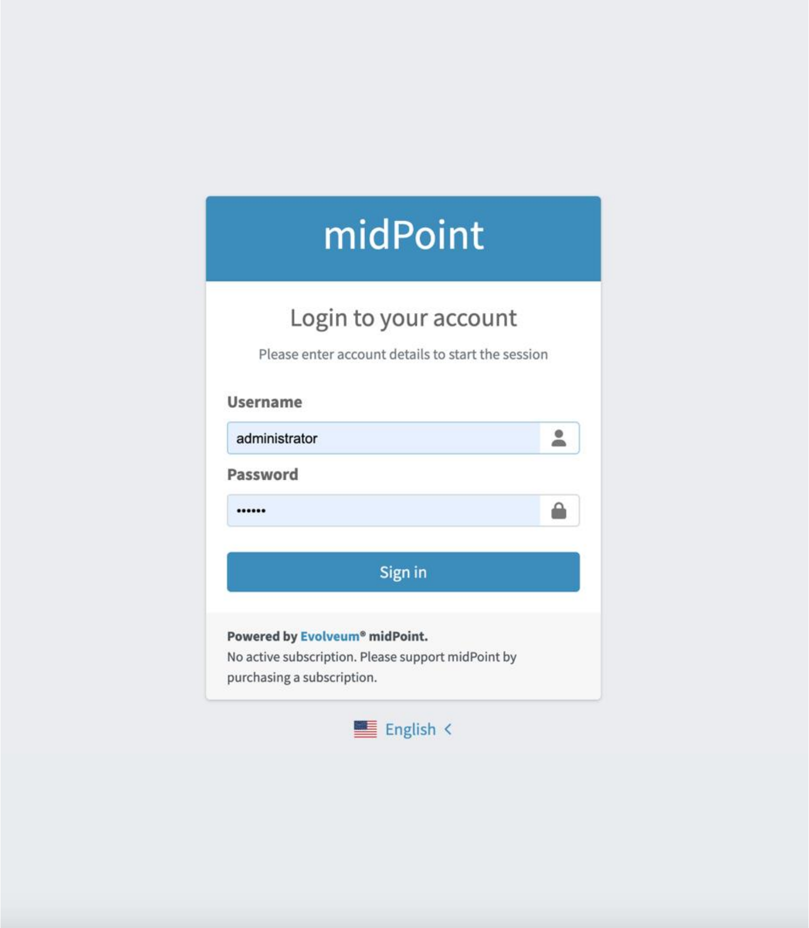
Password: ••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Department Business Access

- **Scenario:** Discover org related roles
  - Based on org unit
  - Focus on Sales, Contractor and Irregular user org unit
  - Includes requestable roles, available for temporary or specialized access based on user needs

NOTE: Try advanced mode and then compare it with already predefined mode for this specific task.



midPoint

Login to your account

Please enter account details to start the session

Username: administrator

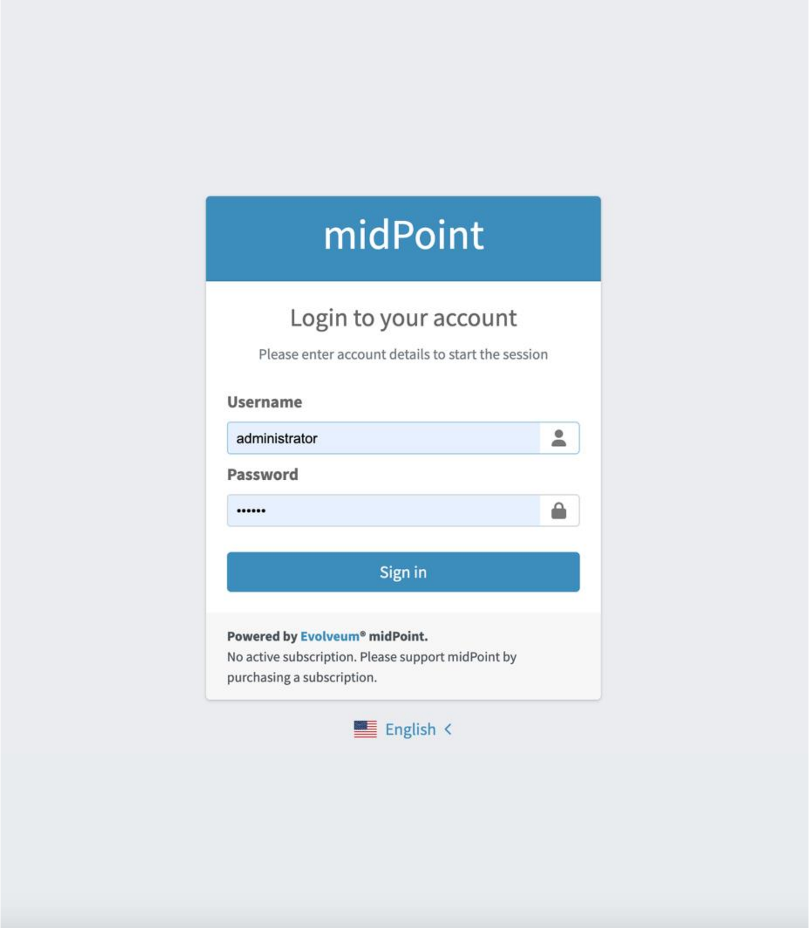
Password: ••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Practical part - Job Business Access

- **Scenario:** Discover job related roles
  - Based on the “title” attribute
  - Tailored for specific job responsibilities and business locations
  - Includes requestable roles, available for temporary or specialized access based on user needs

NOTE: Use an iterative approach to exclude unwanted objects and minimize noise in the cluster. Imagine that job related roles are not marked by an archetype.



midPoint

Login to your account

Please enter account details to start the session

Username: administrator

Password: ••••••

Powered by Evolveum® midPoint.
No active subscription. Please support midPoint by purchasing a subscription.

Key takeaways and applications

Overview of role mining concepts
Role mining approach and how role mining process work.

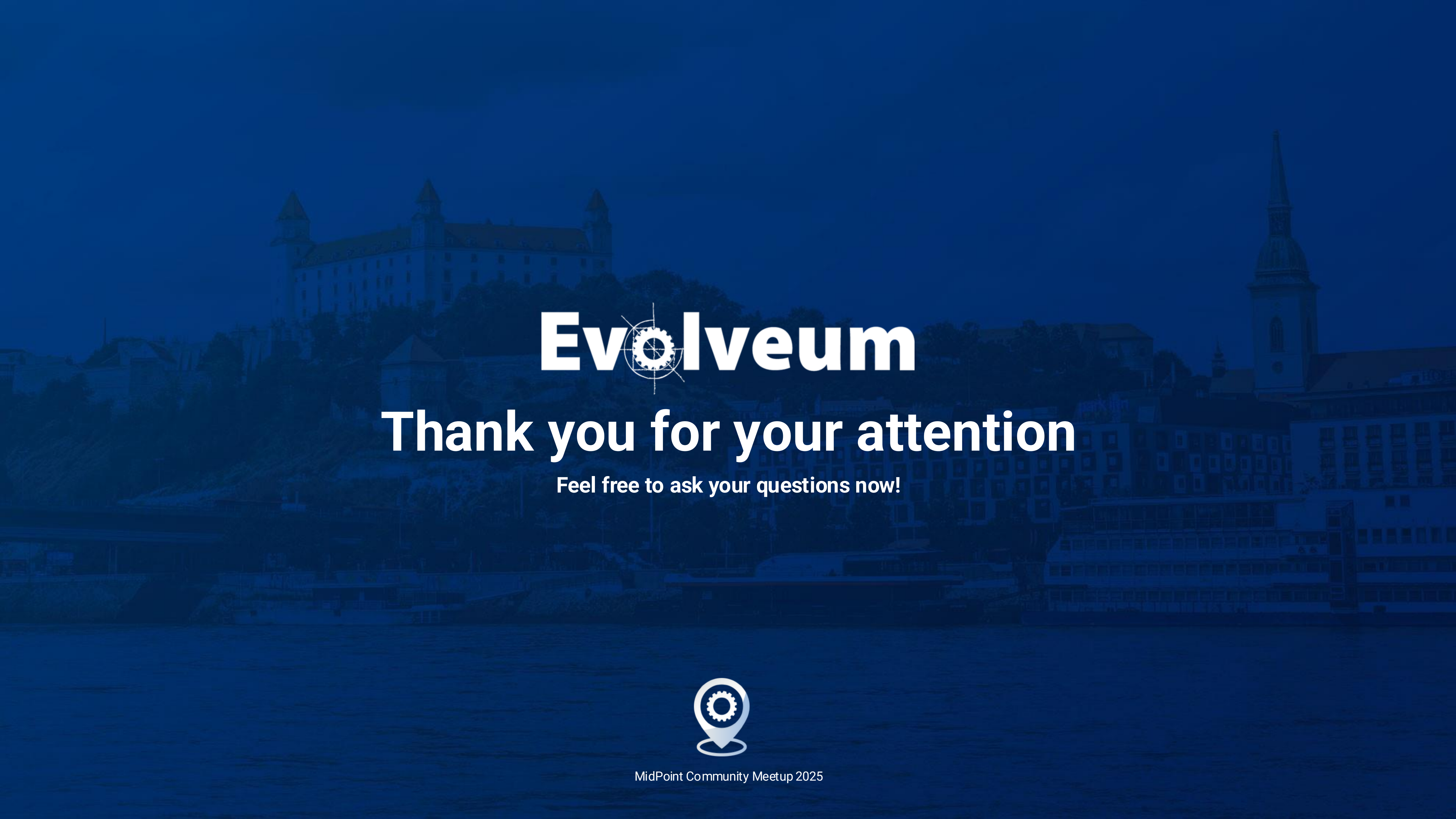
Hands-on exploration
Possibility to understand data structure.
Reduce manual efforts.

Work through different role mining scenarios
Suitable for different type of tasks or scenarios.

Refinement
Switch from complex to structural based business model.

Conclusion

- Role Mining is a powerful tool that improve access control and governance
- Helps in the transition to a business model
- It is a configurable process
- For more information about Role Mining in the midPoint, explore our documentation:
  - https://docs.evolveum.com/midpoint/reference/roles-policies/mining/



Evolveum

Thank you for your attention

Feel free to ask your questions now!

MidPoint Community Meetup 2025