MidPoint Community
Meetup 2025

IGA - Who Has Access to What and Why ?

Martin Špánik

CISO at Evolveum

Evolveum

Agenda

- Phishing attack description
- MidPoint and its capabilities
  - Fast response
  - Recovery
  - Prevention
- Midpoint Example

The Attack

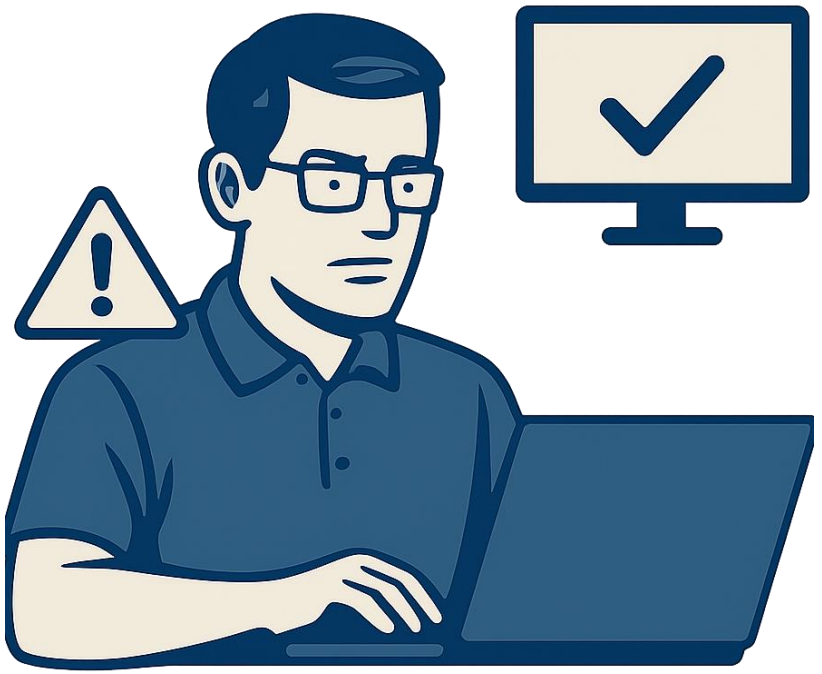
- Phishing campaign in the morning
  - New employee was fooled to enter credentials
- SPAM campaign in the evening
  - Monitoring notification of unusual email activity from our system
  - Notification of the employee of missing emails from sent folder

The Response

- Fast analysis of mail server activity
  - Identify the account
- Block the attacker
  - Block the account
  - Drop all sessions
- Stop the mail server activities

The recovery

- The attack is stopped now
- Know what exactly happened – where the attacker had access
  - Check everything ?
  - Where does he have access ?
- Communication
  - Internal, external
- Checks and cleanup
- Recover user account



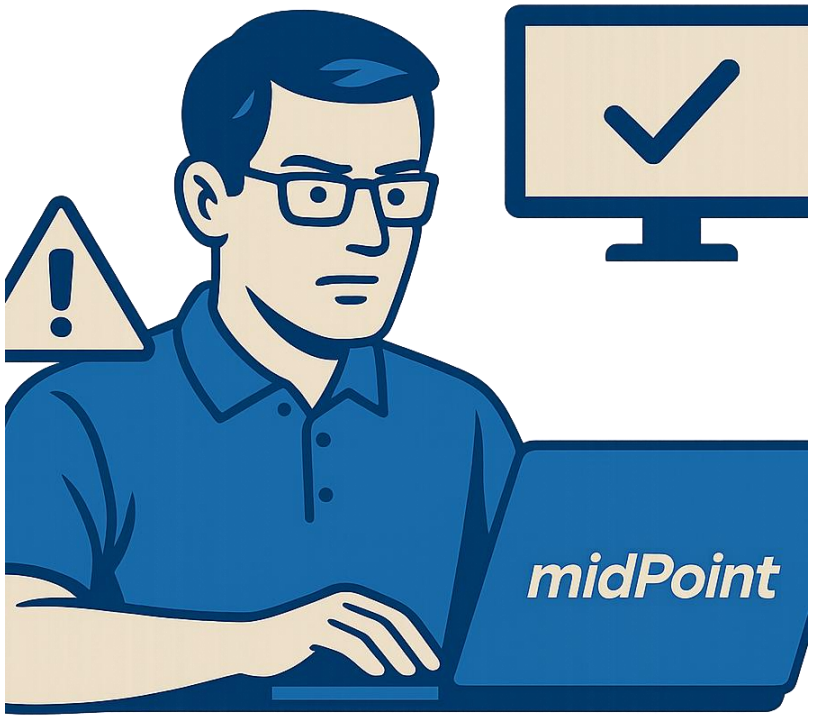
How midPoint can help ?

Fast response

- What accounts does the user have ?
  - Projections
- Change the password (if necessary)
- Block all accounts of the user
  - Centralized: Automatic & Manual
  - Manual tickets identified and can be processed
- Session drop can’t be done by midPoint
  - but you know where exactly it must be dropped

Recovery / analysis

- What accounts does the user have ?
  - Projections on resources
    - Activation status of the accounts
- Where does the user have access ?
  - User access
  - Applications
- What was the last activity of the user ?
  - User history / audit log
  - Access requests…



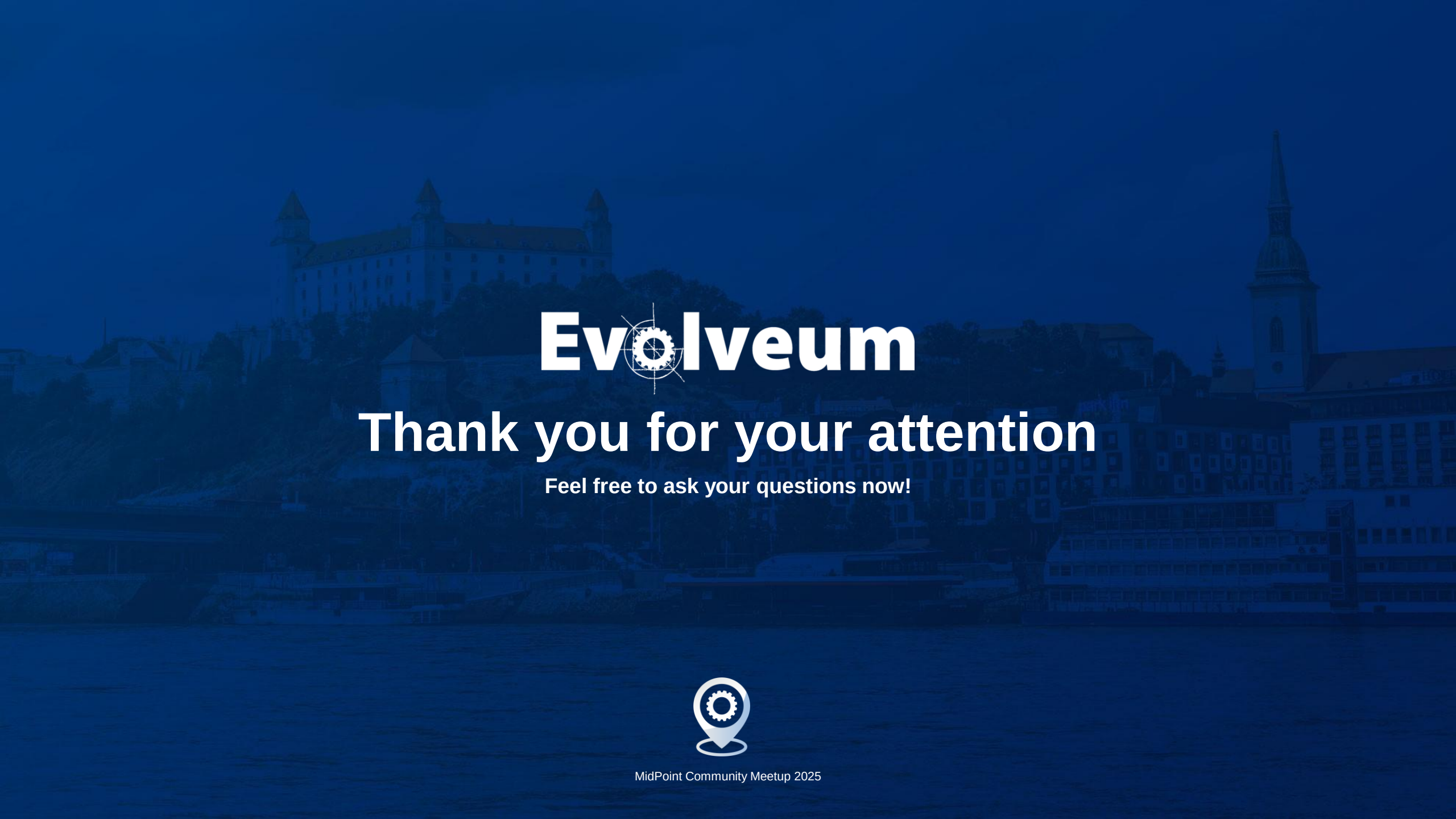
Prevention

- Individual objects
  - Accounts
  - Accesses
  - Applications
- Big picture
  - Dashboards
    - Actual status
    - Suspicious accounts
    - Privileged users…
  - Reports
    - Who has access to what and why ?

Example with midPoint

IGA visibility - Design considerations

- Direct access to accounts
  - Do not build “provisioning chains”
- Coverage
  - Cover the most you can
    - If not automatic, then manual ticketing
- Represent targets
  - Applications
- Use Object marks
  - Perform checks with manual processing


Evolveum
Thank you for your attention
Feel free to ask your questions now!
MidPoint Community Meetup 2025