2nd Annual

MidPoint Community Meetup

Cybersecurity Hide and Seek

May 2026

Martin Špánik
CISO & Compliance

Radovan Semančík
Software Architect

Evolveum

Agenda

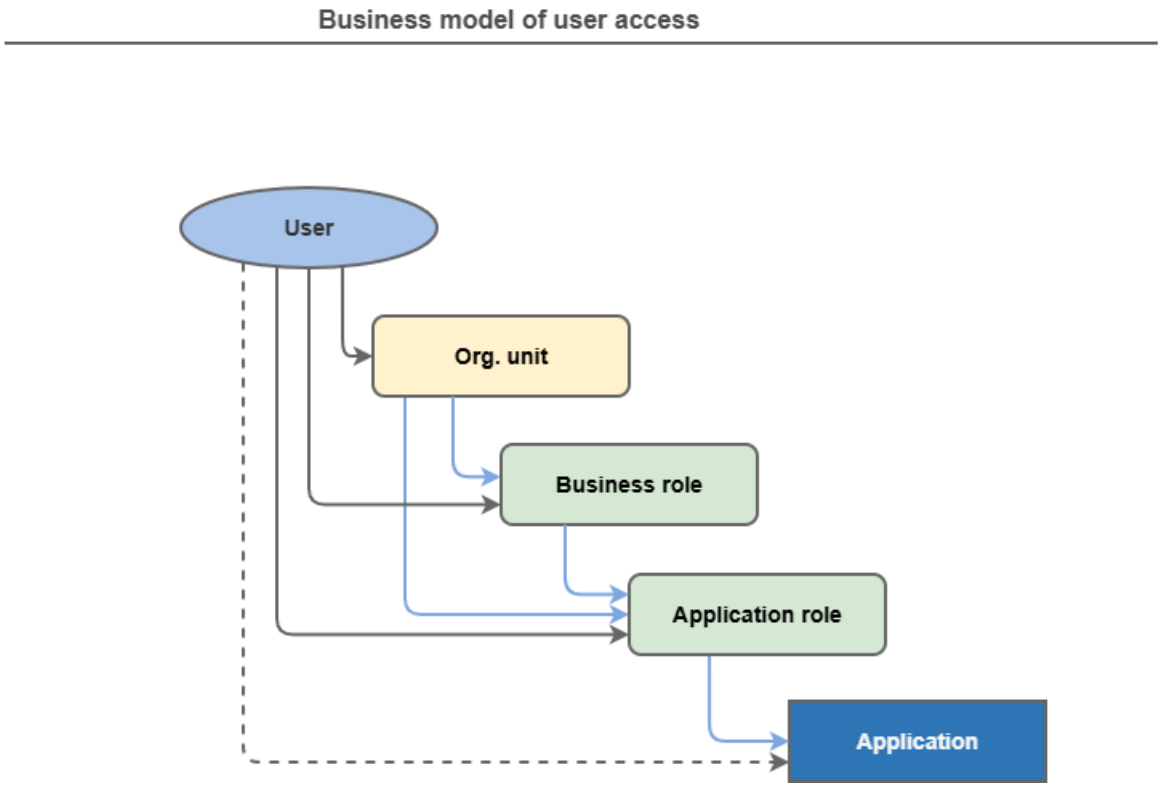
- Visibility
- Users, roles, applications
- Application inventory
- Governance

Visibility

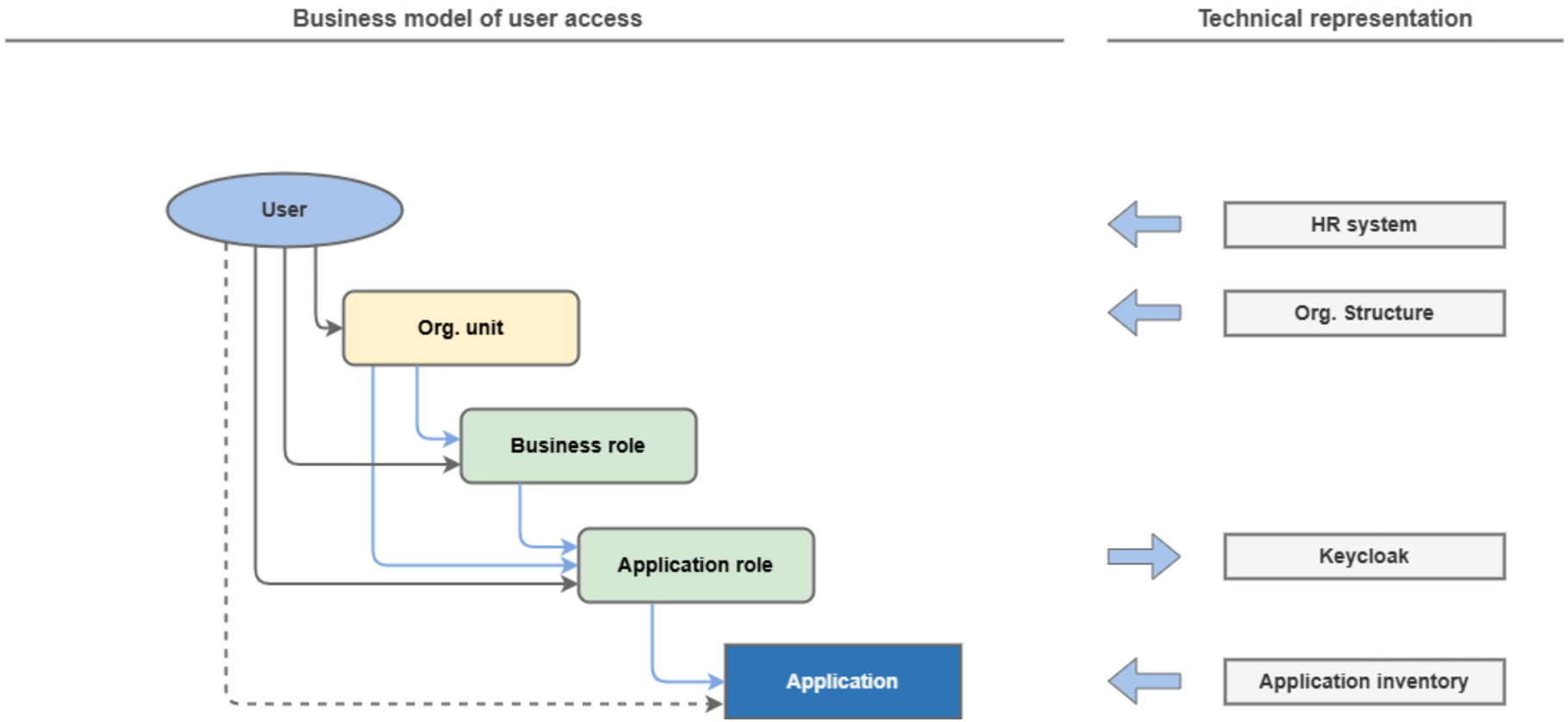
- Visibility: fundamental requirement of cybersecurity
- Knowing what you have is the first step to protect it
- *Who* has *access* to *what* and *why*
- “Application” is a central concept

Users, Roles, Applications and Resources

- Representation of business relation
- Direct and indirect assignments
  - Assignments
  - Inducements
- User has access to Application

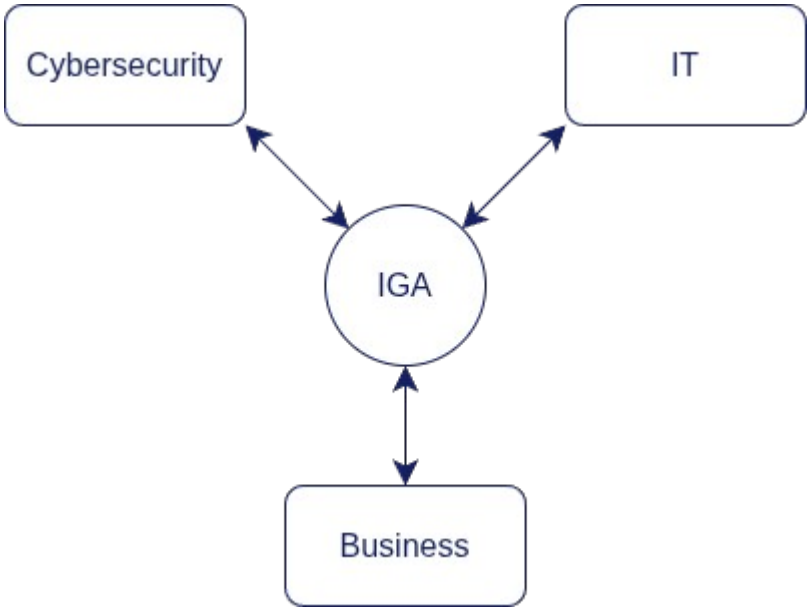


Application vs Resource



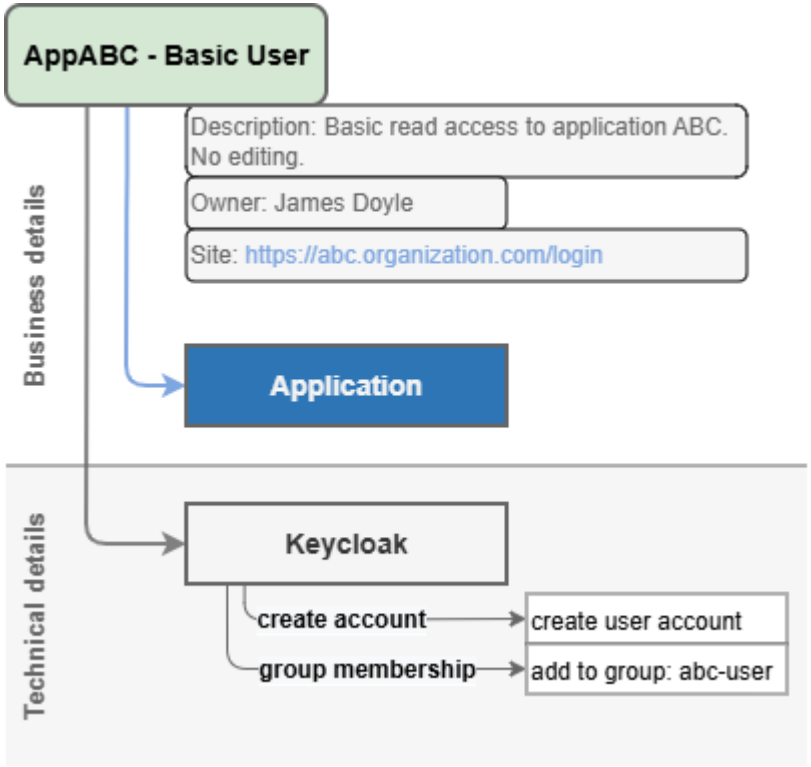
IGA is a Bridge

- Persons – Users – Accounts
- Roles – Groups – Permissions
- Organizational units – Teams – Groups
- Applications – Assets – Namespaces
- Devices – Nodes – Appliances
- Policies – Controls – Rulesets
- Processes – Tasks – Procedures
- Locations – Sites – Zones



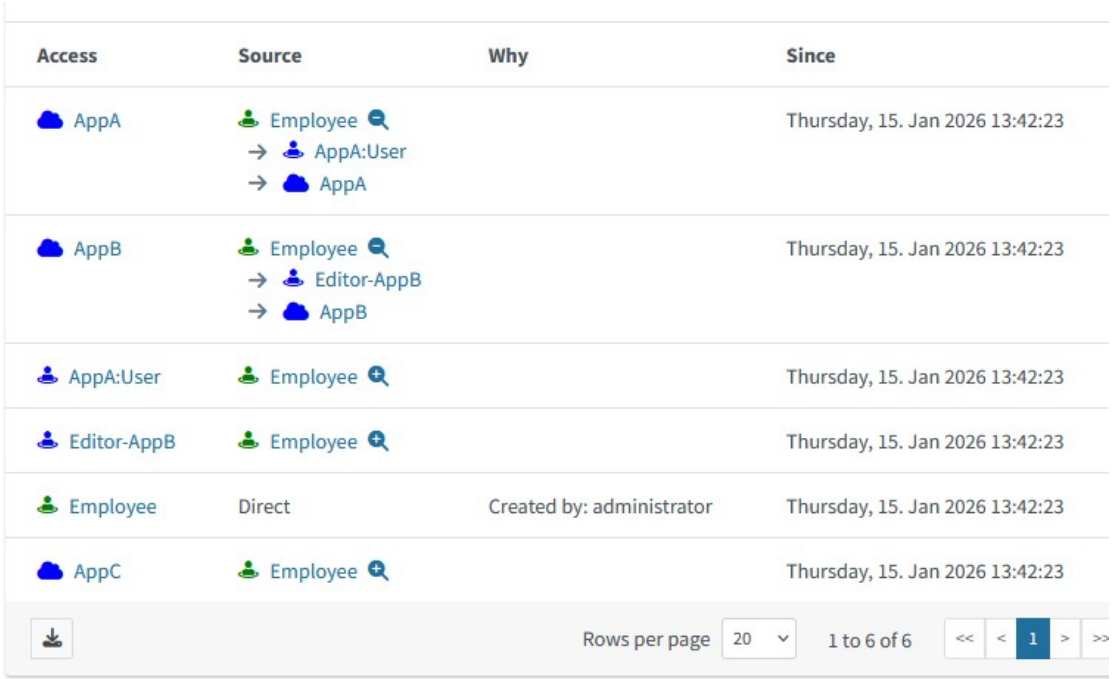
Application Role – Interconnection of Three Worlds

- Application role: **AppABC – Basic User**
  - Basic read access to application ABC. No editing.
    Owned by James Doe.
    Accessible via: https://abc.organization.com/login
  - Providing access to AppABC
  - Create the user account on Keycloak and assign member to group abc-user.
- What is important to users ?
- What is important for provisioning ?
- What is important for security teams ?



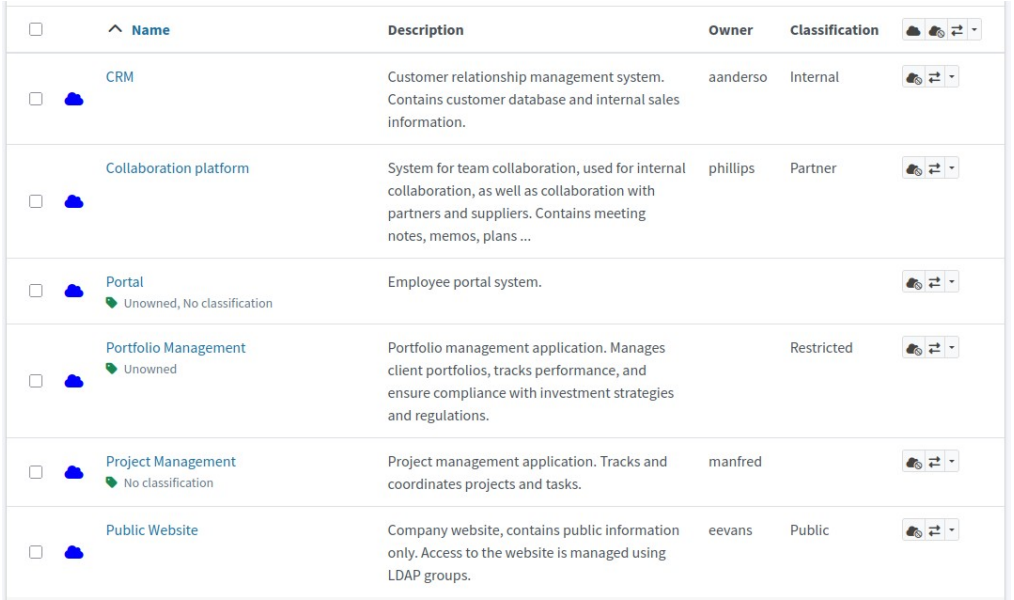
Speak business language

- Business: user / access / application
- Technical: account / entitlement / resource
- Access is manageable by business
  - Access requests
  - Access reviews
- Rules are manageable by business
  - Create business role and assign it to team
  - Add app role to Org unit
- Concept may be extended
  - Add identity, policies, …
- Most important: **Application**



Application Inventory

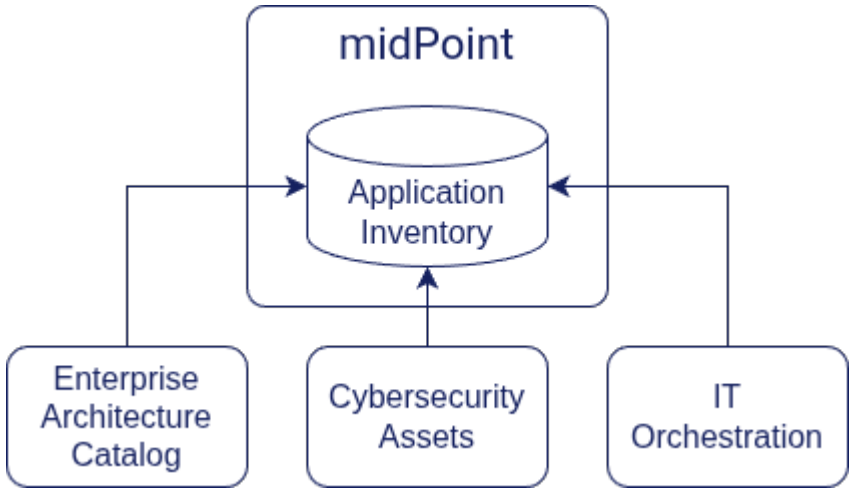
- List of all known applications in an organization
- Application vs Resource
- Live data: actively synchronized
- We want to know about application,
  even if we cannot reach it yet (no *resource*)
- Even more important with instant apps
  (vibe coding)



Name	Description	Owner	Classification
CRM	Customer relationship management system. Contains customer database and internal sales information.	aanderso	Internal
Collaboration platform	System for team collaboration, used for internal collaboration, as well as collaboration with partners and suppliers. Contains meeting notes, memos, plans ...	phillips	Partner
Portal Unowned, No classification	Employee portal system.		
Portfolio Management Unowned	Portfolio management application. Manages client portfolios, tracks performance, and ensure compliance with investment strategies and regulations.		Restricted
Project Management No classification	Project management application. Tracks and coordinates projects and tasks.	manfred	
Public Website	Company website, contains public information only. Access to the website is managed using LDAP groups.	eevans	Public

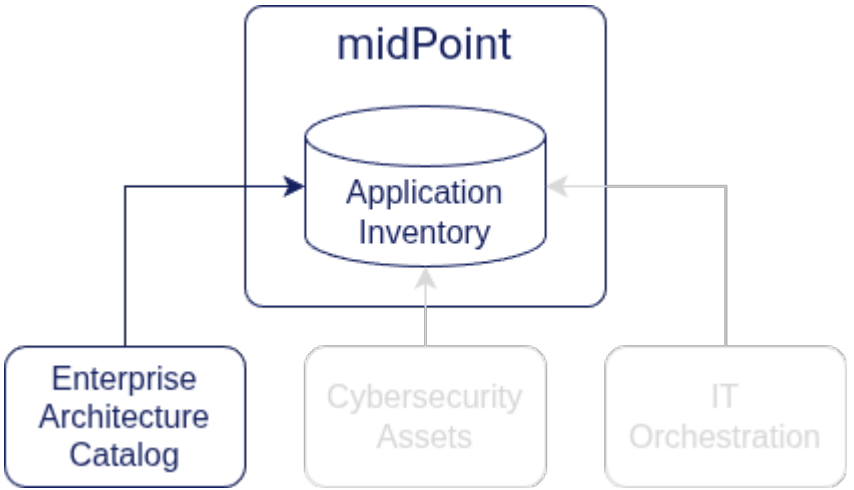
Application Inventory Synchronization

- Generic synchronization mechanism since midPoint 3.0 (2014)
- Synchronization with other application directories
  - Enterprise architecture catalogs
  - IT platforms and orchestration (k8s, Proxmox, etc.)
  - Cybersecurity asset management
- Mapping, correlation, orphan management and everything else



Application Inventory Synchronization Demo

- CSV input, simulating enterprise architecture catalog
- Sync with CSV, discover new apps
  - Correlate to existing app by using identifier (appId)
  - Unmatched apps: create new inventory entry
  - Lifecycle state mapping
- Management of *shadow IT*



https://github.com/Evolveum/midpoint-samples/tree/master/samples/demo/alice

Application Governance

Name	Description	Owner	Classification
CRM	Customer relationship management system. Contains customer database and internal sales information.	aanderso	Internal
Claude Unowned, No classification	Cloud chatbot		
Collaboration platform	System for team collaboration, used for internal collaboration, as well as collaboration with partners and suppliers. Contains meeting notes, memos, plans ...	phillips	Partner
Jabberwock Unowned, No classification	Local AI chatbot		
Portfolio Management Unowned	Portfolio management application. Manages client portfolios, tracks performance, and ensure compliance with investment strategies and regulations.		Restricted
Project Management No classification	Project management application. Tracks and coordinates projects and tasks.	manfred	
Public Website	Company website, contains public information only. Access to the website is managed using LDAP groups.	eevans	Public
SurveyBeast Unowned, No classification	Management of surveys and campaigns		

Application Governance

- Application owners & classification
- Compliance policies
  - Require owner
  - Require classification
- Compliance dashboard
- Application catalog links

Conclusion

- IGA is a bridge: IT – Cybersecurity – Business
- Speak *business* language
- *Application* is a key concept
- Inventory is crucial:
  you cannot protect it if you do not know that you have it
- Governance is the ultimate goal

Evolveum

Thank you for your attention

Feel free to ask your questions now!

2nd Annual MidPoint Community Meetup