

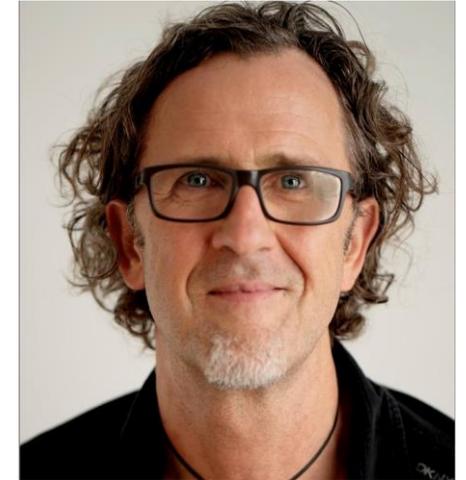
secIT **by heise**

HANNOVER **2024**

Zero Trust Identity – Administrative Aufgaben schützen

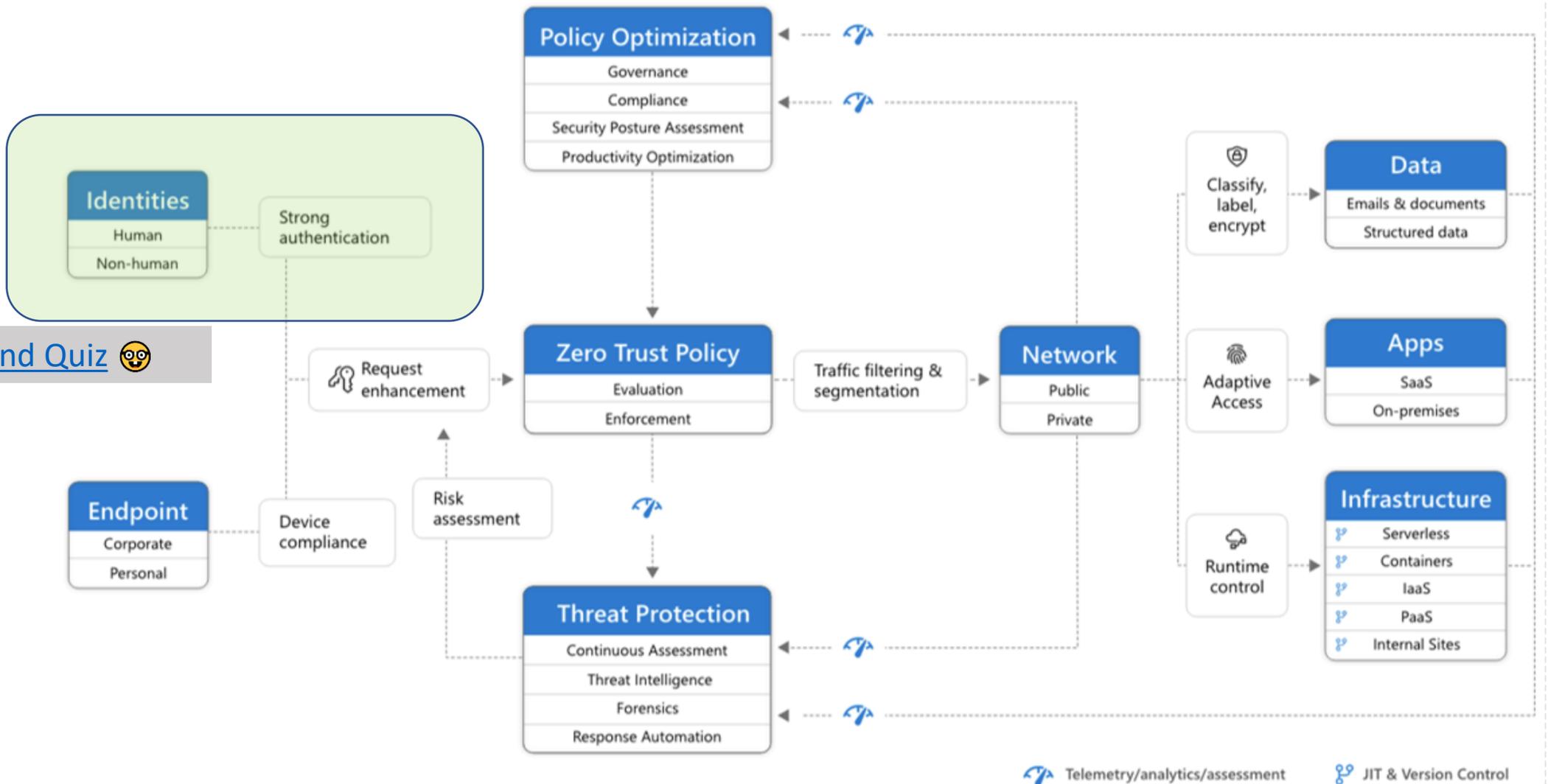
Über mich:

- Zuhause bin ich in Murnau am Staffelsee (45min südlich von München)
- Director Consulting Expert bei CGI Deutschland
- Weitere Stationen: T-Systems International, Wipro
- Schwerpunkte: Active Directory, Identity im hybriden Kontext, Synchronisation und Zero Trust Identity
- Wenn es meine Zeit erlaubt publiziere ich Beiträge in meinem Blog, in der Fachpresse und in der



Blog:
<https://nothingbutcloud.net/>

Zero Trust Identity – Administrative Aufgaben schützen

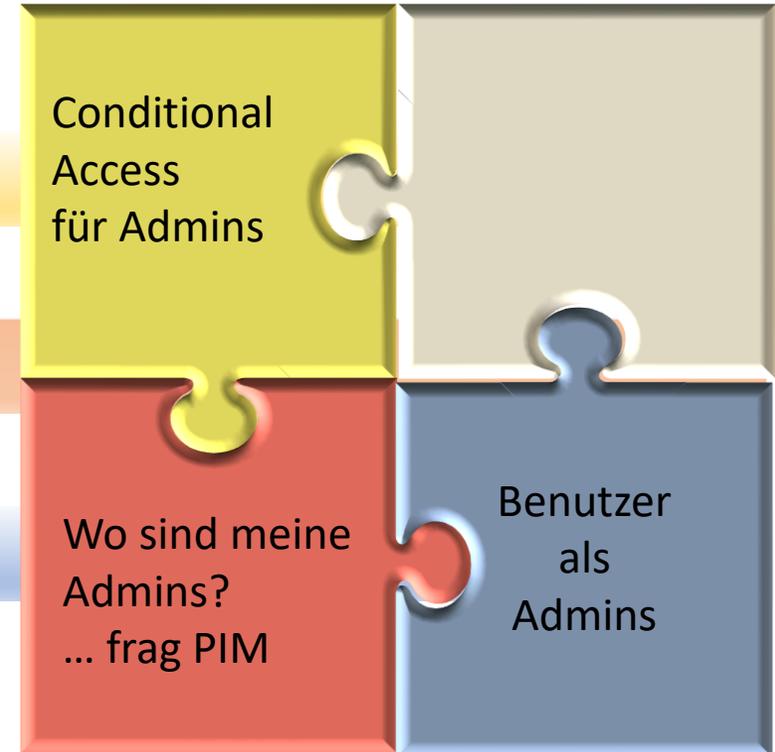


[Mehr Infos und Quiz](#) 🤖

Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

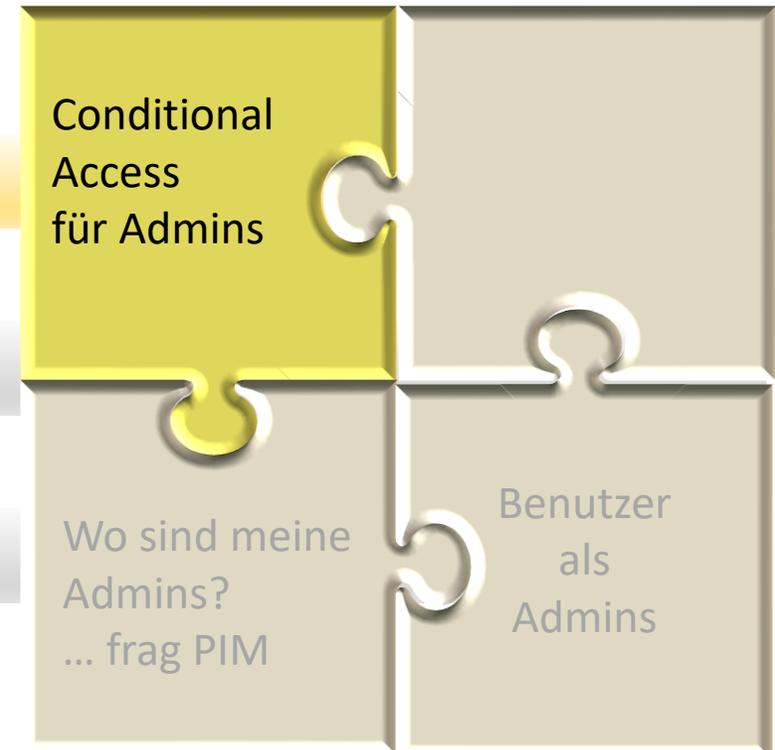
- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken



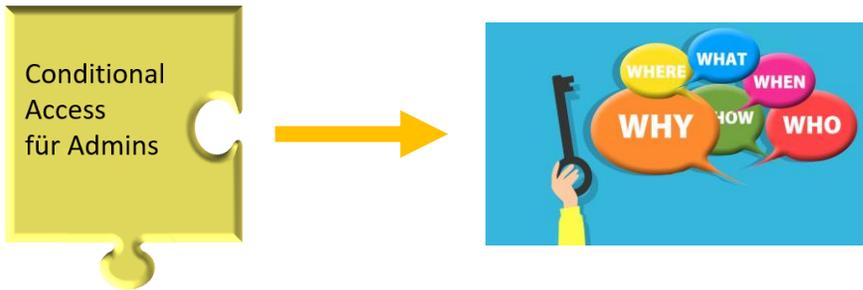
Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken

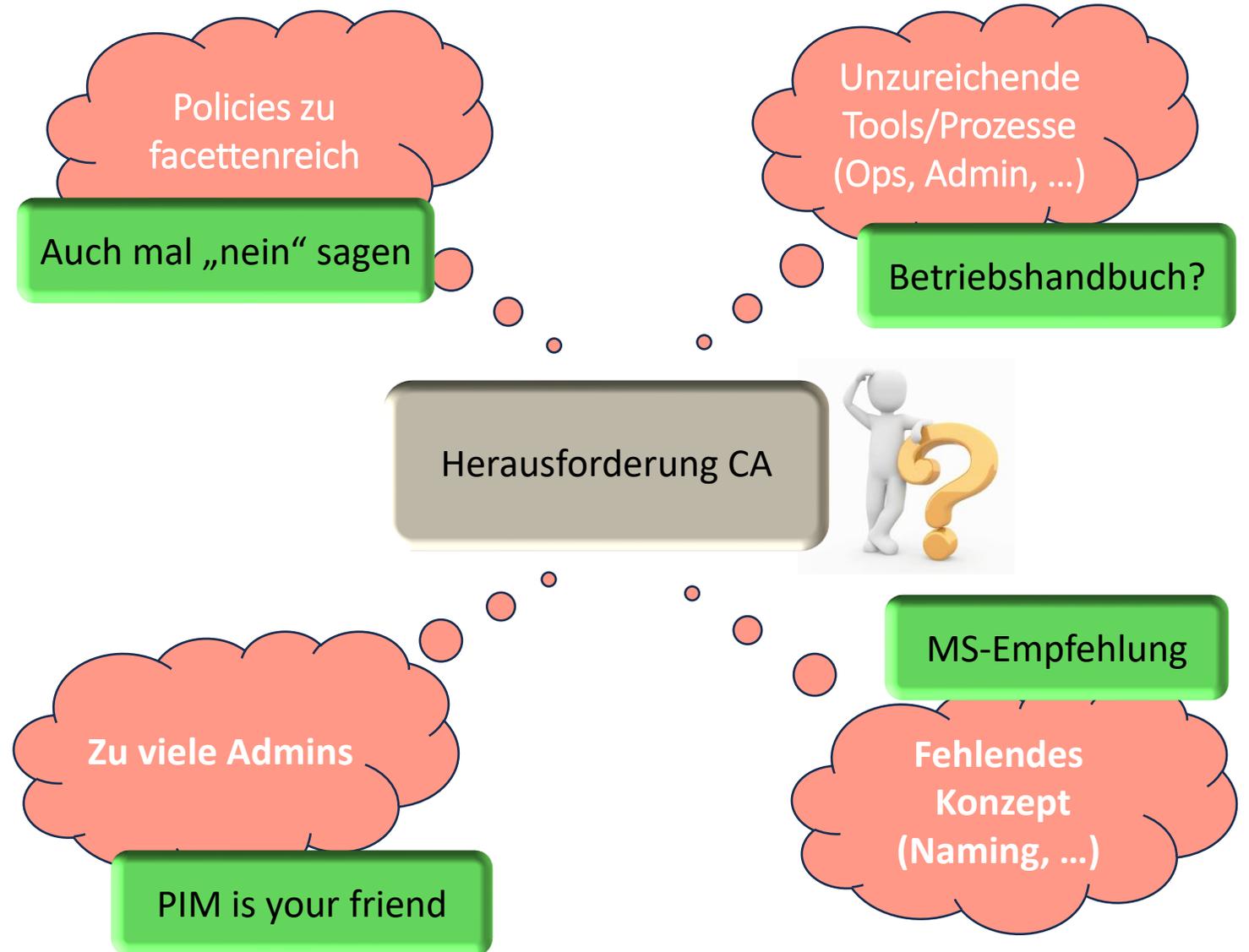


Zero Trust Identity – Administrative Aufgaben schützen



Strategien

- „Keep it simple“
- Tools: Backup, Vergleich etc. z.B. M365DSC, AADInternals
- PIM: Just-in-time (JIT) just-enough-access (JEA)
- Agieren statt reagieren



Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

Empfehlung: Gutes „Naming“ ✓

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation pane includes sections like 'Manage' and 'Troubleshooting + Support'. The main content area is titled 'Klaus Admin | Sign-in logs' and shows a table of user sign-ins. Below this, the 'Activity Details: Sign-ins' pane is open, displaying a table of Conditional Access policies. The table has columns for Policy Name, Grant, Session, and Result. The policies listed include various protection and compliance rules.

Policy Name	Grant	Session	Result
CA001-Global-BaseProtection-AllApps-AnyPlatform-BlockNonPersonas	Block		Not Applied
CA002-Global-BaseProtection-AllApps-AnyPlatform-SessionLifetime12h		Sign-in freq...	Success
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA			Disabled
CA004-Global-Compliance-AllApps-AnyPlatform-CompanyTermsPage	CA_Update...		Not Applied
CA005-Global-Compliance-MarketingApps-AnyPlatform-MarketingTermsPage	TermsPage...		Not Applied
CA006-Global-BaseProtection-AllApps-Android-Block	Block		Not Applied
CA006-Global-BaseProtection-AllApps-AnyPlatform-BlockLegacy	Block		Not Applied
CA100-Admins-BaseProtection-AllApps-AnyPlatform-MFAAuthStrengthPasswordless			Disabled
CA101-Admins-BaseProtection-AllApps-AnyPlatform-SignInFreqNonPersistent		Sign-in freq...	Success
CA103-GradyAdmin-CAProtection-Mac_Safari_CA_Delete_Protection-Block			Not Applied
CA400-GuestUser-BaseProtection-AllApps-AnyPlatform	Require m...		Not Applied
CA500-Developer-Compliance-AllApps-AnyPlatform-DeveloperTermsPage	CA_Update...		Not Applied



Must read:
[Conditional Access framework and policies - Azure Architecture Center | Microsoft Learn](#)

Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

Empfehlung: Protected Actions ✓

Home > Conditional Access

Conditional Access | Authentication contexts

Microsoft Entra ID

- Overview
- Polices
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- Authentication contexts**
- Authentication strengths
- Classic policies

Get started **Authentication contexts**

Manage authentication context to protect data at Conditional Access policies. [Learn more](#)

Name

Admin compliant

Home > Conditional Access | Policies >

CA103-GradyAdmin-CAProtection-Mac_Safari_CA_Delete_Prot...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to

Name * Authentication context

CA103-GradyAdmin-CAProtection-Mac_Saf...

Assignments

Users

Specific users included and specific users excluded

Target resources

1 authentication context included

Conditions

1 condition selected

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. [Learn more](#)

Select the authentication contexts this policy will apply to

Admin compliant

CA Policy

Home > Privileged Identity Management | Microsoft Entra roles > Identity LAB | Roles >

Edit role setting - Attack Payload Author

Privileged Identity Management | Microsoft Entra roles

Activation Assignment Notification

Activation maximum duration (hours)

8

On activation, require

None

Azure MFA

Microsoft Entra Conditional Access authentication context

[Learn more](#)

Admin compliant

Label for Admin compliant computer

PIM Role

+ Add protected actions Refresh Manage view Remove Preview features Got feedback?

Protected actions enable permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action. [Learn more](#)

Search by name or description

3 actions found

Permission	Description	Conditional Access authentication context
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for Conditional Access policies	Admin compliant
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/create	Create Conditional Access policies	Admin compliant
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/delete	Delete Conditional Access policies	Admin compliant

Zero Trust Identity – Administrative Aufgaben schützen

Conditional
Access
für Admins

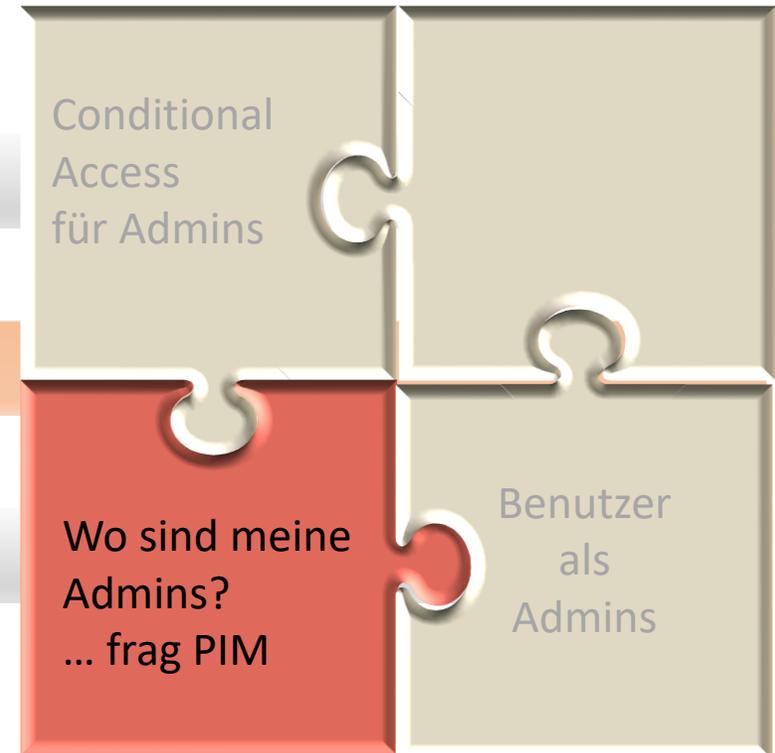
Demo :
Conditional Access Policies
for Admins



Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken



Zero Trust Identity – Administrative Aufgaben schützen

Strategien

Wo sind meine Admins?
... frag PIM

PIM - kurz und bündig

Workflows für Rollenaktivierung

Konfig für jede Rolle

MFA oder Protected Action je Rolle

Aktivieren über PIM-Dashboard PS / Graph

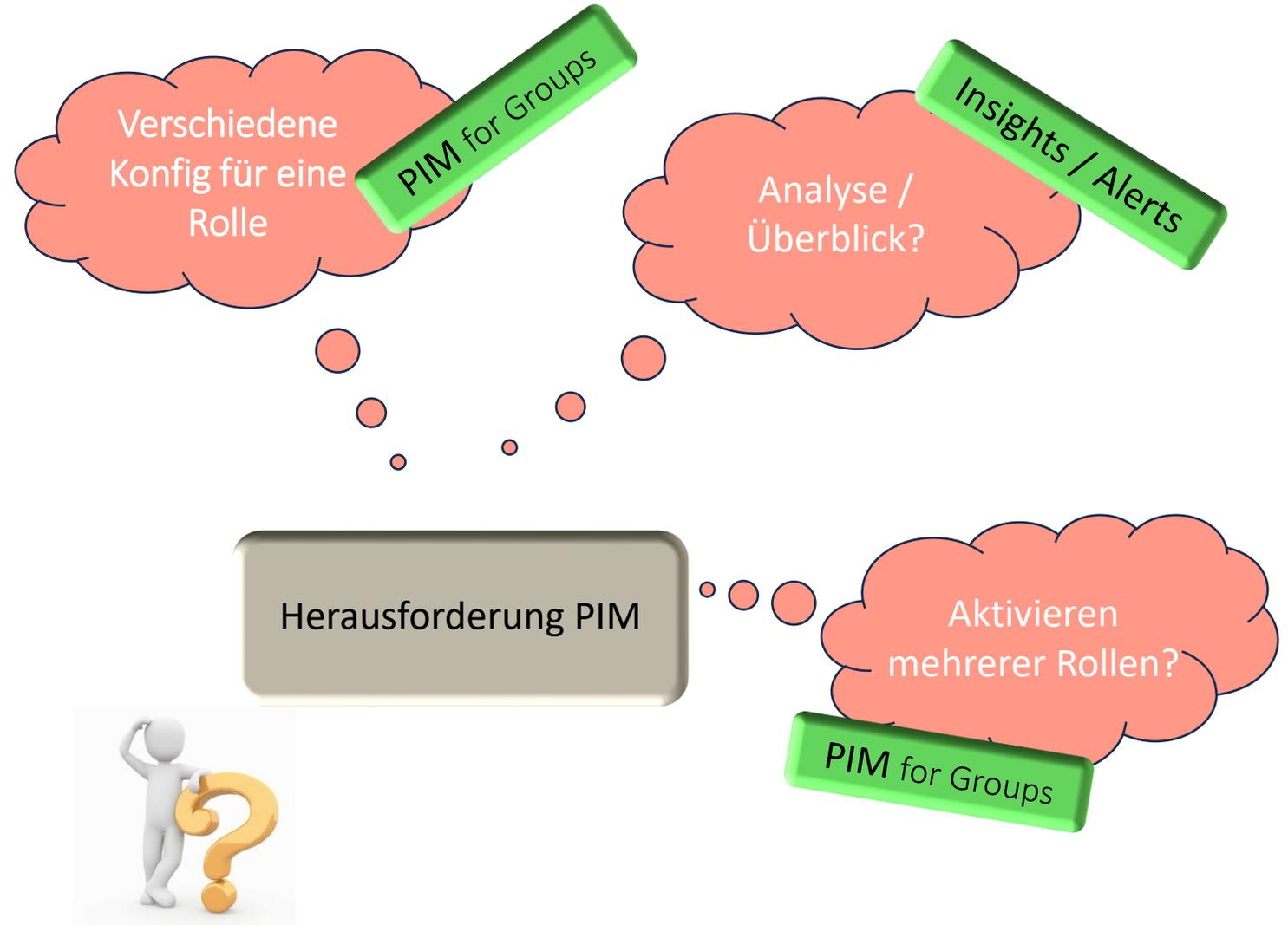
P2 für alle User die an PIM teilnehmen

Integration in Access Reviews

Umfassende Notification bei Rollenaktivitäten

Konfig für Entra Rollen, Gruppen und IaaS

Analyse kritischer Rollen



Zero Trust Identity – Administrative Aufgaben schützen

Wo sind meine
Admins?
... frag PIM

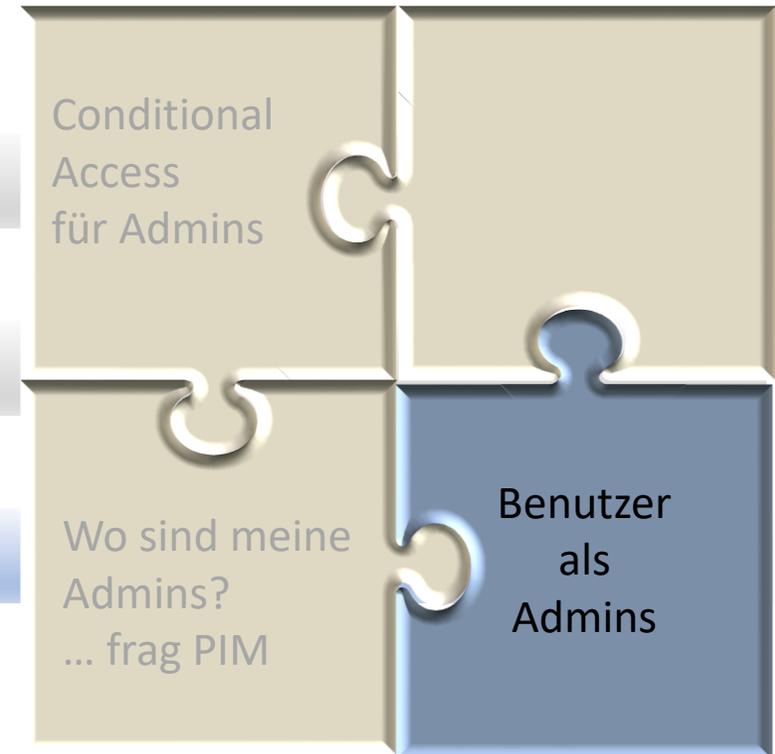
Demo :
PIM for Groups



Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken



Zero Trust Identity – Administrative Aufgaben schützen



Das Wichtigste rund um „Administrative Units“

Management auf bestimmte Objekte reduzieren

Administrativer Kontext für Benutzer, Gruppen und Geräte

Keine hierarchische Struktur oder Verschachtelung. Keine Vererbung

PowerShell, Graph API, Entra Admin Center, MyStaff und M365 Admin Portal

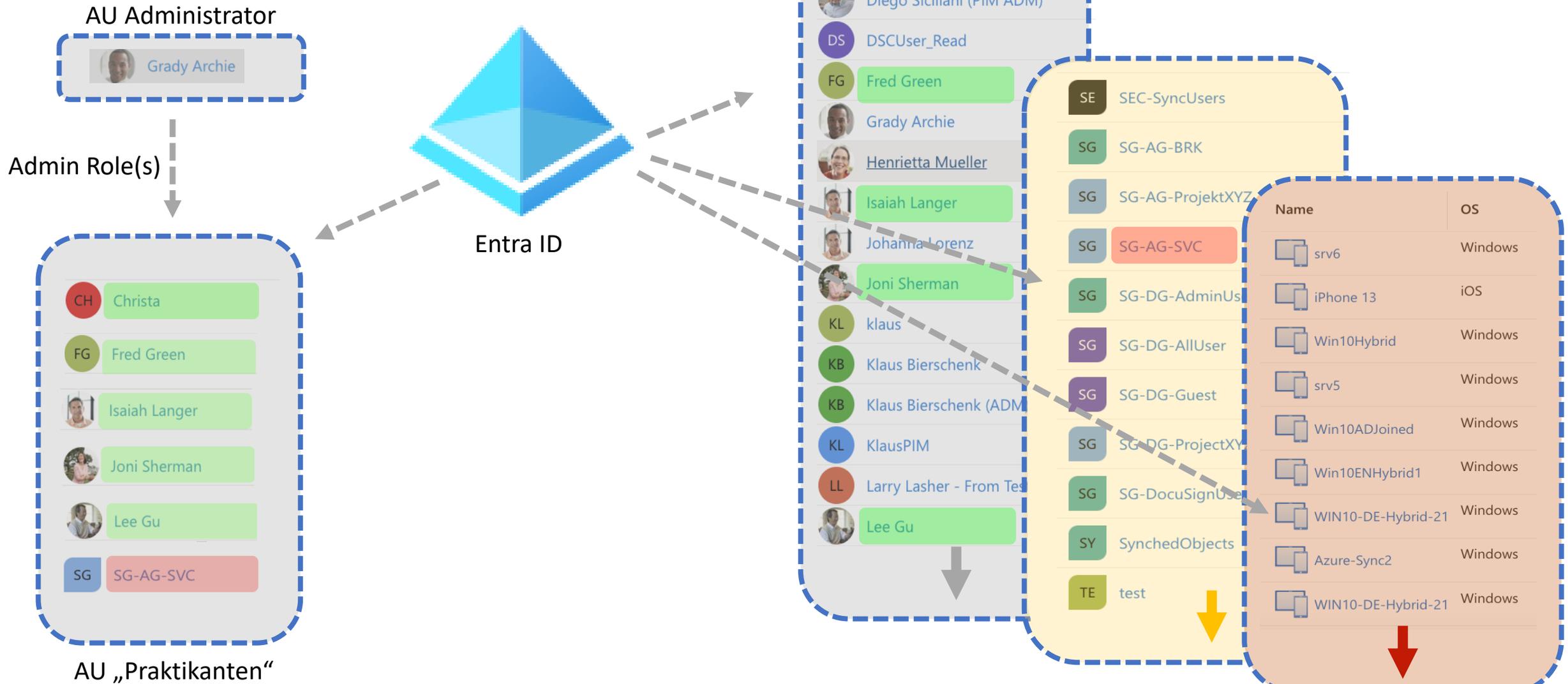
MyStaff bietet „einfache“ administrative Möglichkeiten (PW Reset)

Objekte können mehreren „Administrative Units“ zugeordnet sein

Nicht verwechseln mit Organizational Units (OUs) aus den AD Domain Services

Zero Trust Identity – Administrative Aufgaben schützen

Beispiel für Administrative Units (AU)



Zero Trust Identity – Administrative Aufgaben schützen



Demo :
Administrative Units



Zero Trust Identity – Administrative Aufgaben schützen

Die drei wichtigsten Vorteile und Herausforderungen zu „Administrative Units“



Vorteile:

Administrative Möglichkeit für Benutzer ohne Zugriff auf das Entra Admin Center

Implementierung ohne viel Aufwand. Gut geeignet für kurzfristigen Zweck (Projekt)

Management für bestimmte Benutzer (keine Admins) ermöglichen. Einfaches Toolset

Herausforderungen:

Mehrere AUs werden schnell unübersichtlich. Wer darf was und wo ist schnell unklar

Nur einige wenige Rollen sind verfügbar. Und nicht alles ist möglich (siehe [Link](#))

Keine Schachtelung möglich, um Hierarchien aufzubauen

Zero Trust Identity – Administrative Aufgaben schützen

Grundlagen

- [Zero Trust Model - Modern Security Architecture | Microsoft Security](#)
- [Was ist der bedingte Zugriff in Microsoft Entra ID?](#)
- [Was ist Microsoft Entra Privileged Identity Management?](#)
- [Administrative Unit Verwaltungseinheiten in Microsoft Entra IDs](#)
- [Emergency Access \(BGA Accounts\)](#)
- [Dynamic Group Membership](#)
- [MFA - how it works](#)



Weiterführende Informationen

- [Framework und Richtlinien für bedingten Zugriff - Azure Architecture Center | Microsoft Learn](#)
- [Privileged Identity Management \(PIM\) für Gruppen](#)
- [NothingButCloud: BGA Alerting](#)

Tools

- [What is Microsoft365DSC?](#)
- [Entra Exporter Tool - Effortlessly Backup Microsoft Entra ID Configurations \(o365reports.com\)](#)

secIT by heise

HANNOVER 2024



Zero Trust Identity – Administrative Aufgaben schützen

Backup

Zero Trust Identity – Administrative Aufgaben schützen



Empfehlung:

Tools ✓



Microsoft365DSC

Export, Backup, Vergleich von Einstellungen schwierig

M365SDC: Sichern, Vergleichen, Automatisieren und mehr ...

Powershell- und DSC-Kenntnisse sind hilfreich

Community Lösung mit gutem Support (Github)

Keine reine Backup / Restore Lösung

PS-Modul mit ca. 60 Cmdlets



Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

Empfehlung:

Authentication strength ✓



Microsoft Entra admin center

Search resources, services, and docs (G+)

Conditional Access | Policies

CA100-Admins-BaseProtection-AllApps-AnyP

Conditional Access policy

Delete View policy information

Name *

CA100-Admins-BaseProtection-AllApps-Any...

Assignments

Users

Specific users included and specific users excluded

Target resources

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Enable policy

Report-only On Off

Save

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

Warning: "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength

Passwordless MFA

Info: To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor

Select