AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

IT-Security Deep Dive

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Automatisierung von Sicherheitslösungen gezeigt an BeyondTrust PRA

Michael Brändli
Security Engineer,
AVANTEC

AVANTech-Day 2026

Michael Brändli
Security Engineer,
AVANTEC

...seit Juni 2019 bei der AVANTEC AG (FLS Team)

...seit Mai 2023 im PAM & Access Security Team

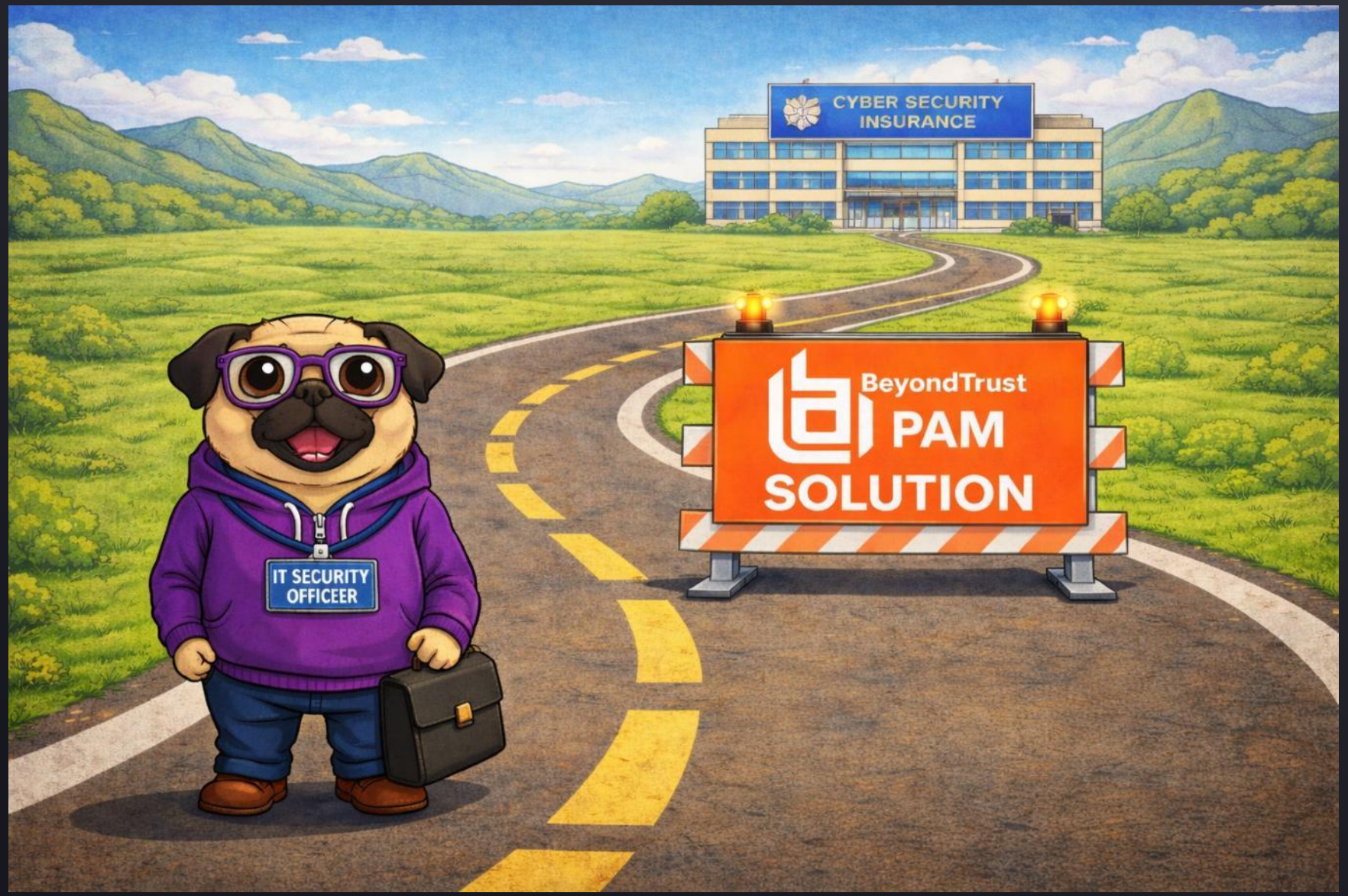
Inhalt

AVANTEC
Competence. Security. Trust.

- Die Reise
- Kurze Einführung BeyondTrust PRA
- Zu konfigurierende Komponenten
  - Mögliches Problem
- Automatisierung
- Demo
- Kunden Case – Viega (Dominic Welsch)
- Q&A

Die Reise

AVANTEC
Competence. Security. Trust.



Kurze Einführung PRA

Privileged Remote Access

AVANTEC
Competence. Security. Trust.

BeyondTrust
Platform

Kurze Einführung PRA

Privileged Remote Access

AVANTEC
Competence. Security. Trust.

Privileged Remote Access

Remote Support

Kurze Einführung PRA

Privileged Remote Access

AVANTEC
Competence. Security. Trust.

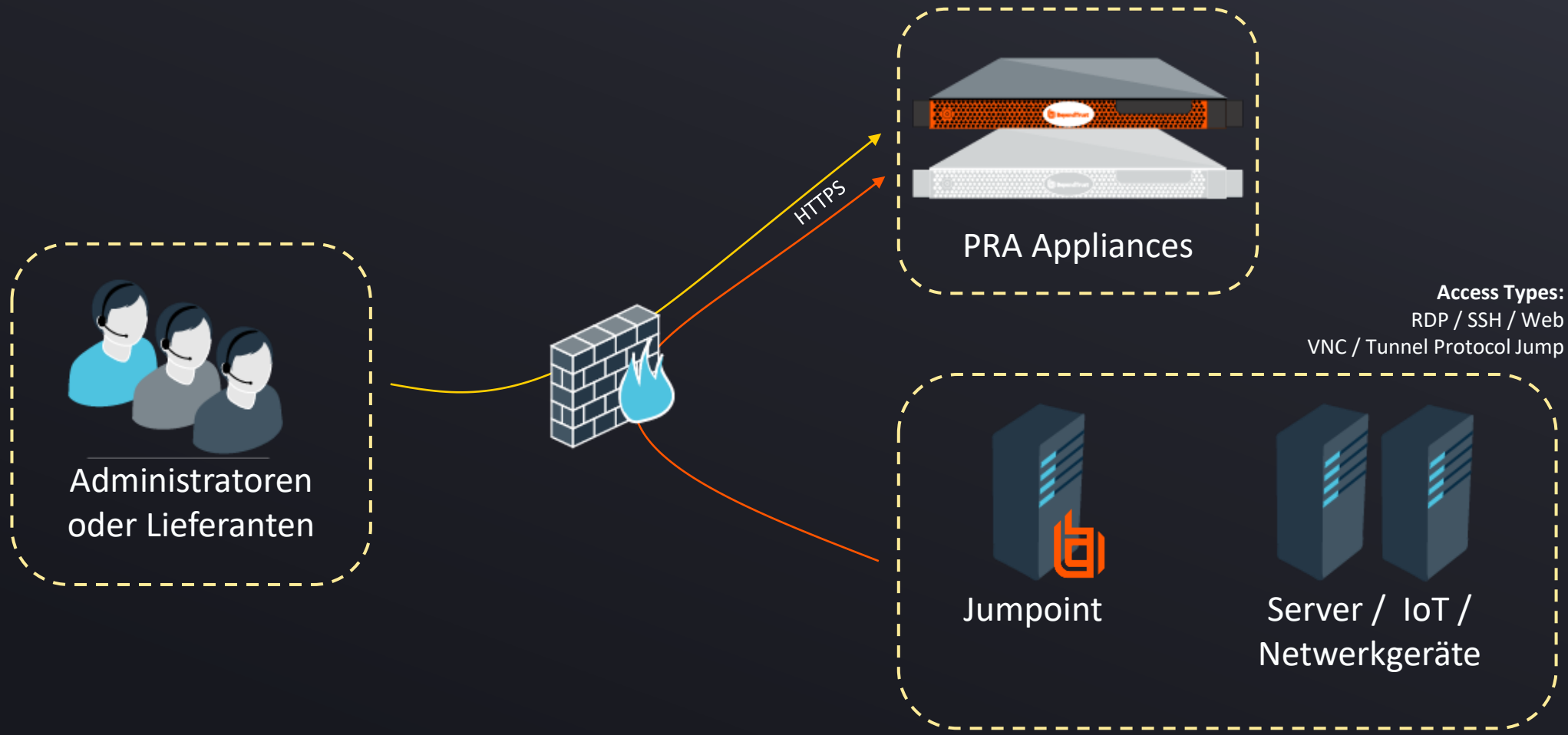
Interne IT

Lieferanten

Kurze Einführung PRA

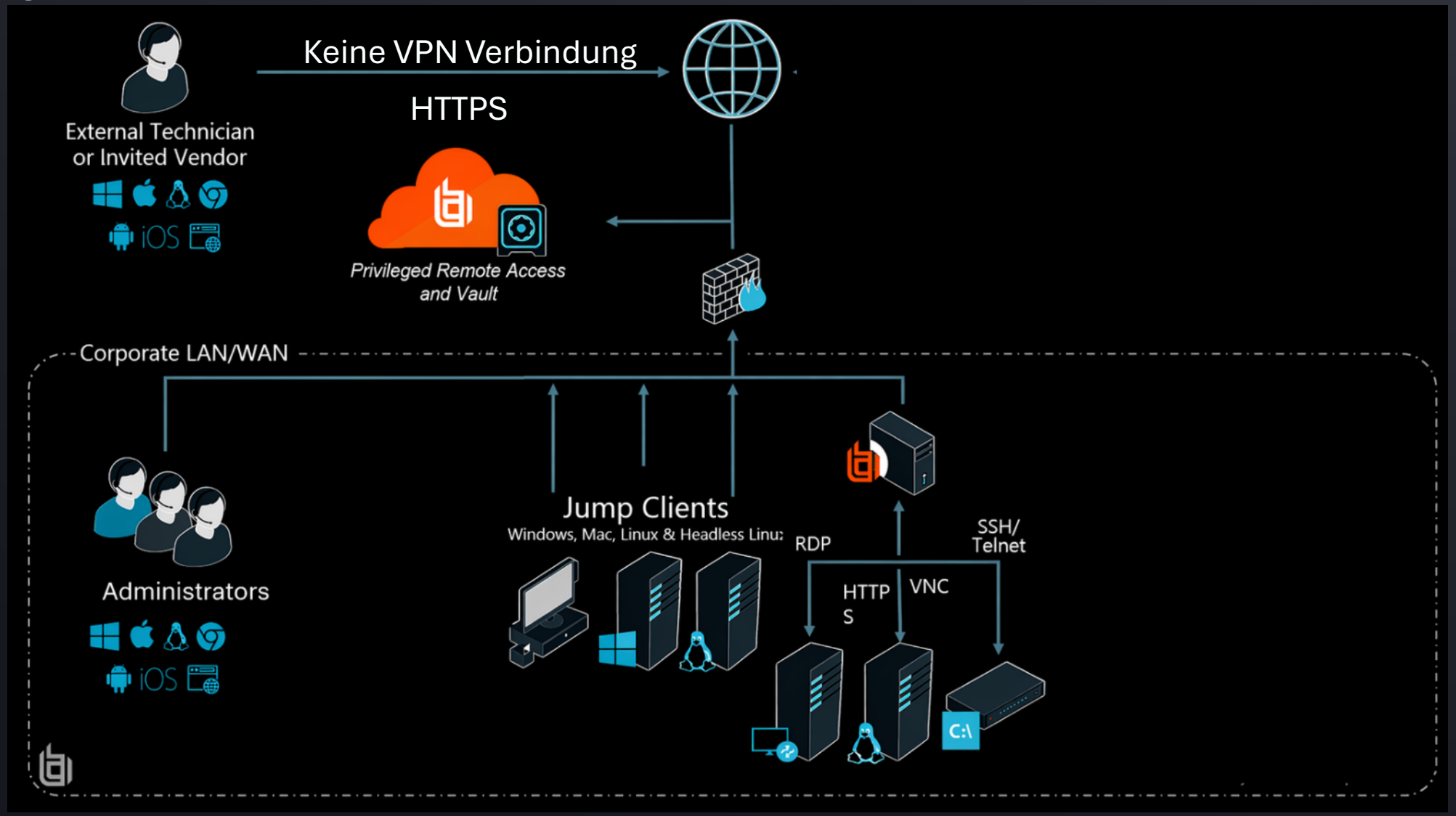
Privileged Remote Access

AVANTEC
Competence. Security. Trust.



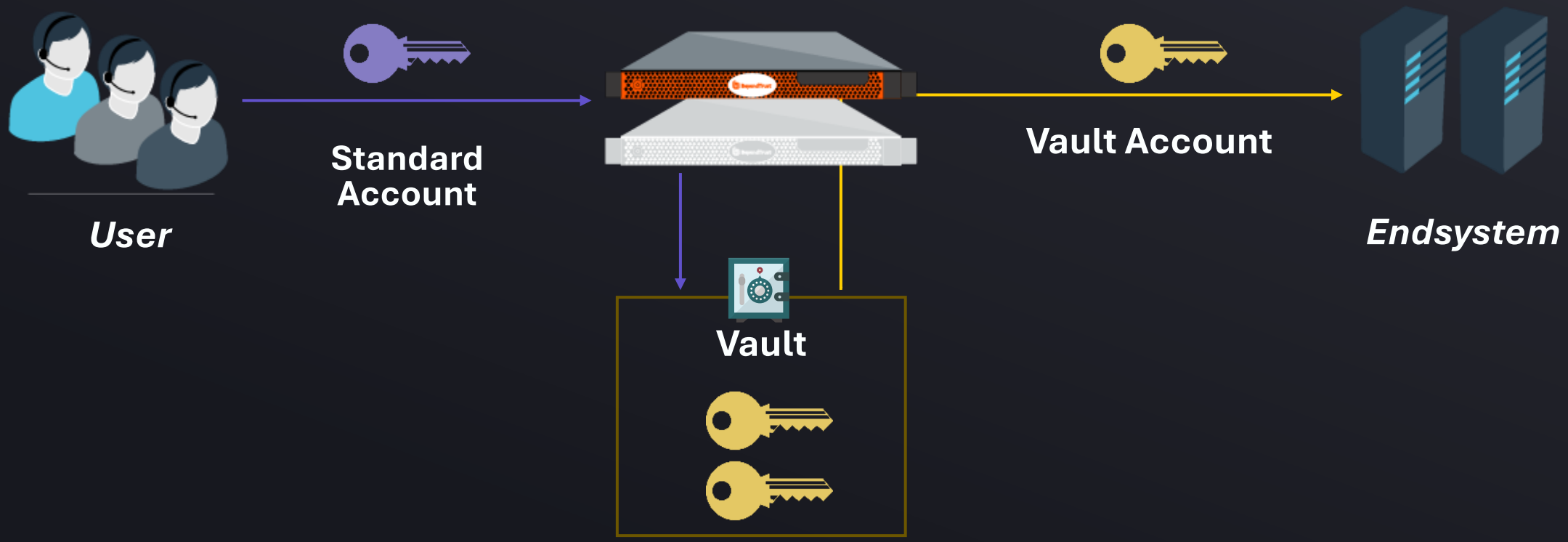
Kurze Einführung PRA

Privileged Remote Access



Kurze Einführung PRA

Privileged Remote Access - Accountwechsel



Zu konfigurierende Komponenten

Einmalig

Was	Beschreibung
Date & Time	Zeit & Datum
Access Session Logging Settings	Recording der Access Sessons
Jump Client Installer	MSI für Jump Client Installation
Jumpoint (Gateway)	Installation Jumpoint(s)
Domain Onboarding	Anbinden von On-Prem AD / EntraID
Email Configuration	Versand von Mails (Session Invite, System Info…)
Site Configuration	Mind. Passwortlänge, Standard IdP. …

Zu konfigurierende Komponenten

Wiederkehrend pro User / Endsystem / Zugriff

Was	Beschreibung
(Erstellung & Zuweisung) User	Anlegen der Standard User
(Erstellung & Zuweisung) Teams	Teams-Funktionalität (Member, Lead, Manager)
(Erstellung & Zuweisung) Jump Client / Jump Item	Anbindung Endsystem
(Erstellung & Zuweisung) Jump Groups	Logische Sortierung der Endsysteme Berechtigen auf Endsysteme
(Erstellung & Zuweisung) Jump Policy	Berechtigungen, bevor eine Session startet
(Erstellung & Zuweisung) Session Policy	Berechtigungen während einer Session
(Onboarding & Zuweisung) Vault Account	Vault Account für Zugriff auf das Endsystem
(Erstellung & Zuweisung) Group Policy	Zentraler Ort für Zuweisung der Berechtigungen

Zu konfigurierende Komponenten

AVANTEC
Competence. Security. Trust.

Automatisierung?

AVANTEC
Competence. Security. Trust.

Automatisierung

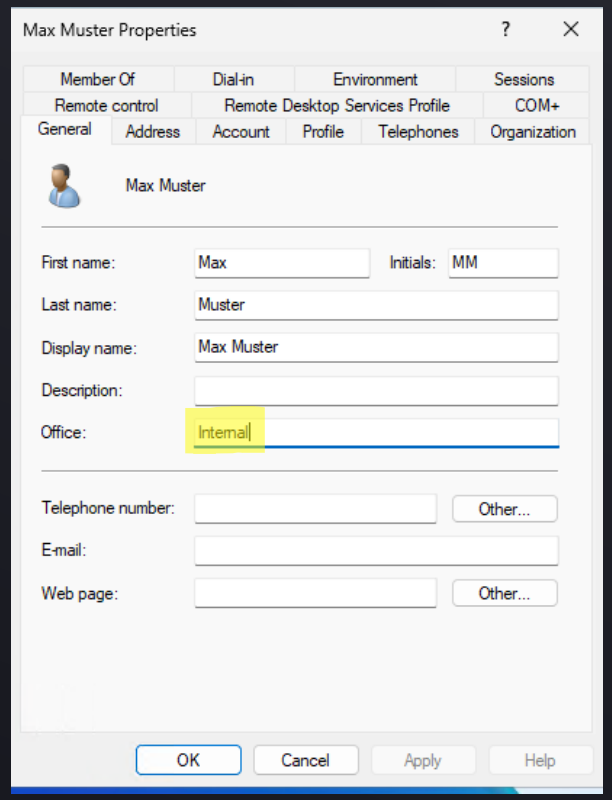
AVANTEC
Competence. Security. Trust.

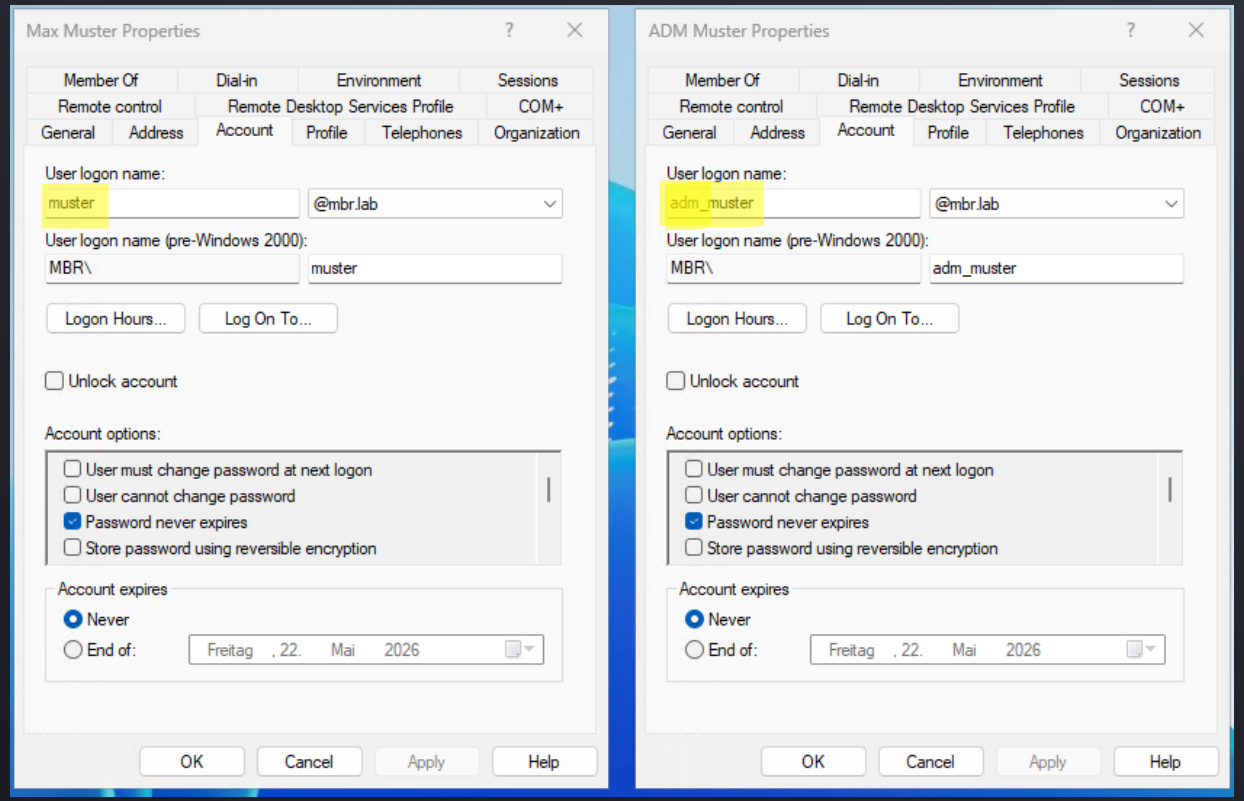
- Alle Informationen stehen (bereits) im AD / EntraID
- Allgemeine Security Group für Provisionierung auf PAM-Lösung
- Zuweisung von User zu Endsystemen über Security Groups
- Ableiten von Standard Account auf Vault Account
  - max_muester@mbr.lab -> *adm_*max_muester@mbr.lab
- Attribute für
  - Internal / External
  - Team: Member / Lead / Manager

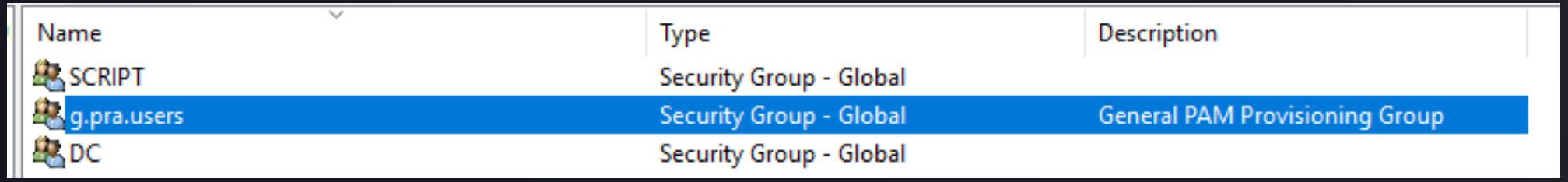
Ziel: Alle zu konfigurierenden Info's müssen irgendwo stehen ☺

Automatisierung

AVANTEC
Competence. Security. Trust.







Automatisierung

IT Admins

Administrieren

Domain Controller

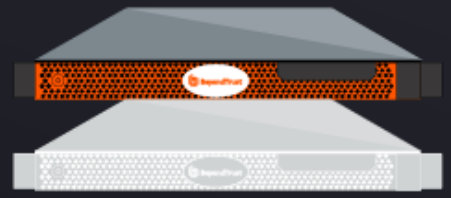
auslesen

Schedule

Script

Automation Server

(C)REATE / (R)EAD / (U)PDATE / (D)ELETE



PRA

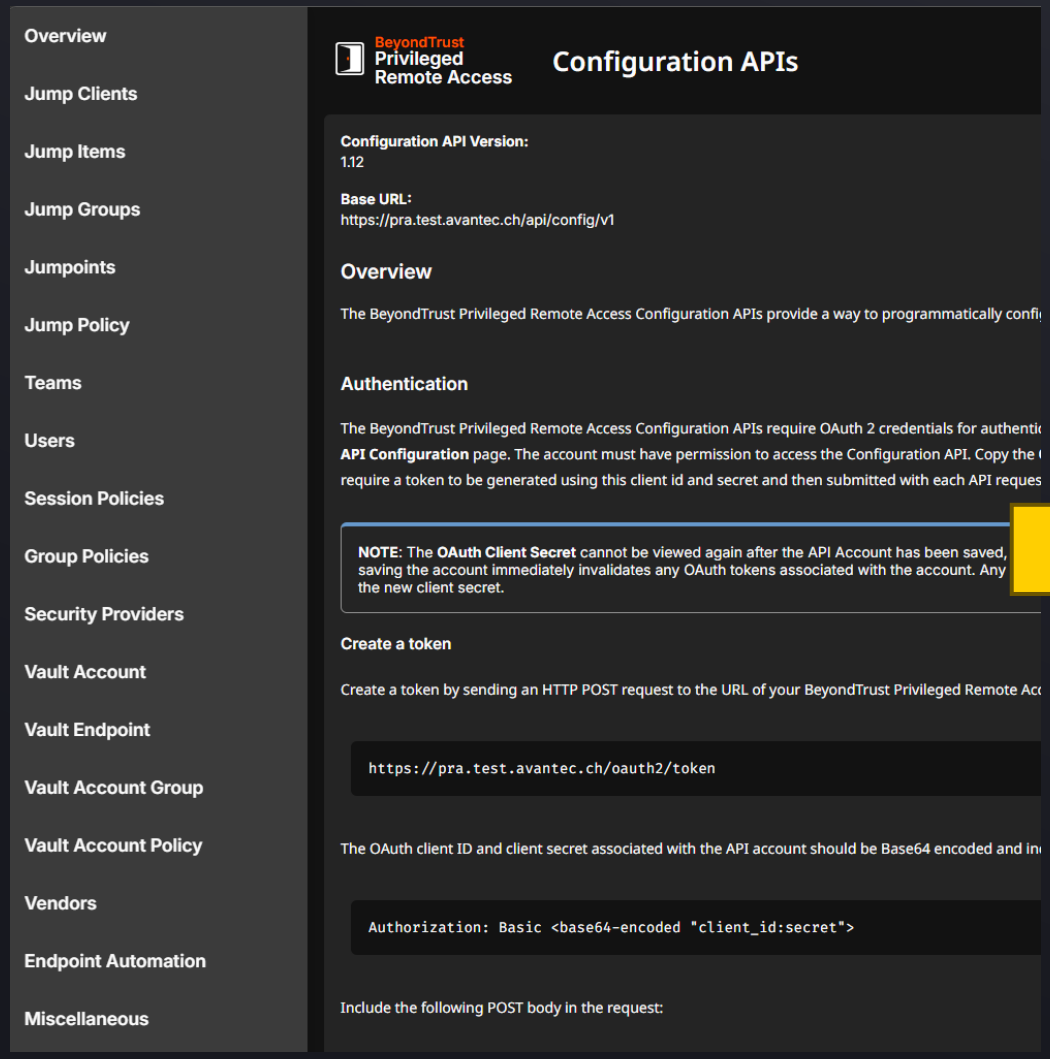
SRA PS Module

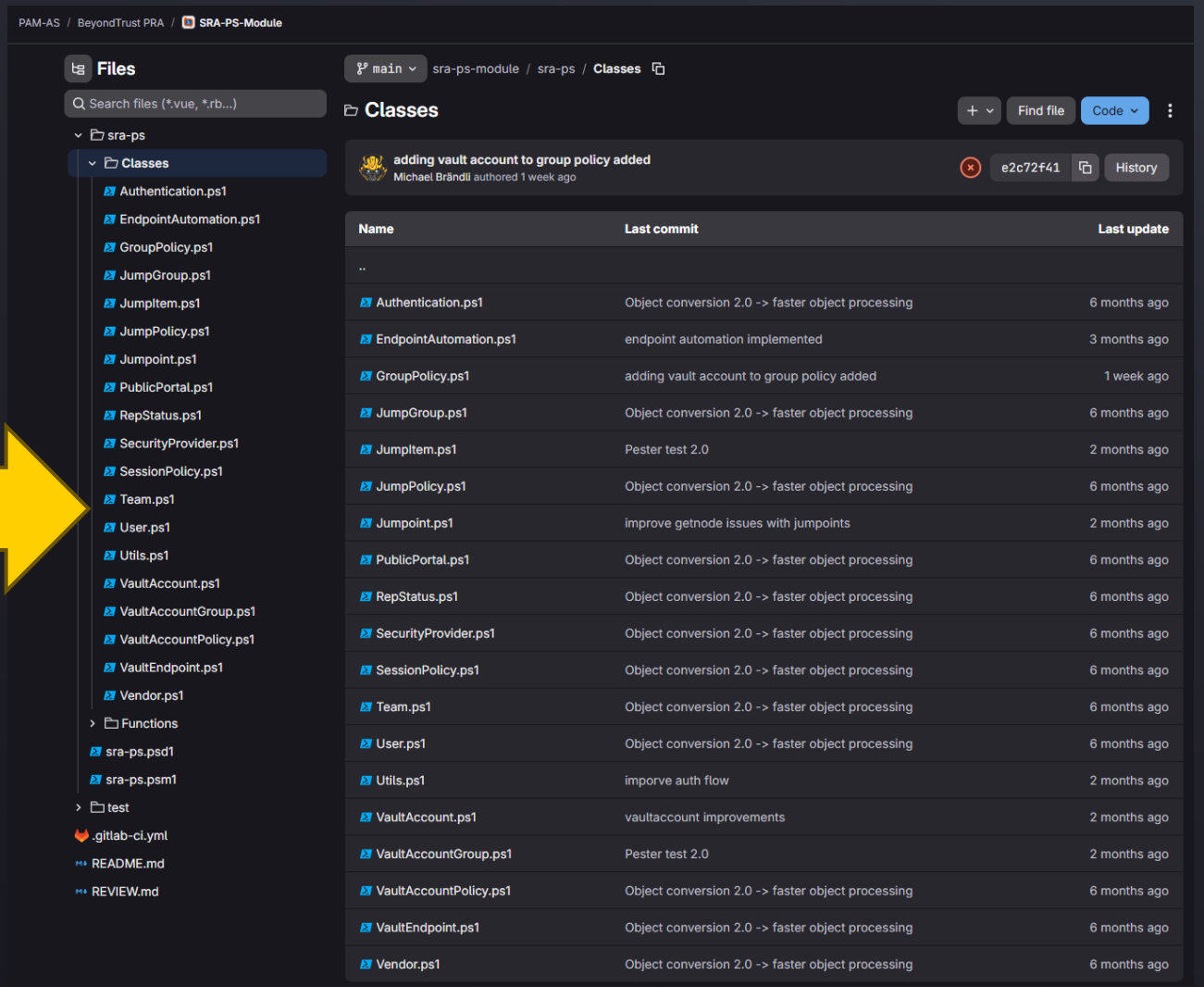
Was ist das?

- Custom PowerShell Module von AVANTEC
- Wiederverwendbares Paket
  - Funktionen
  - Cmdlets
  - Variablen
- (Fast) ganze SRA API abgebildet

SRA PS Module

Was ist das?



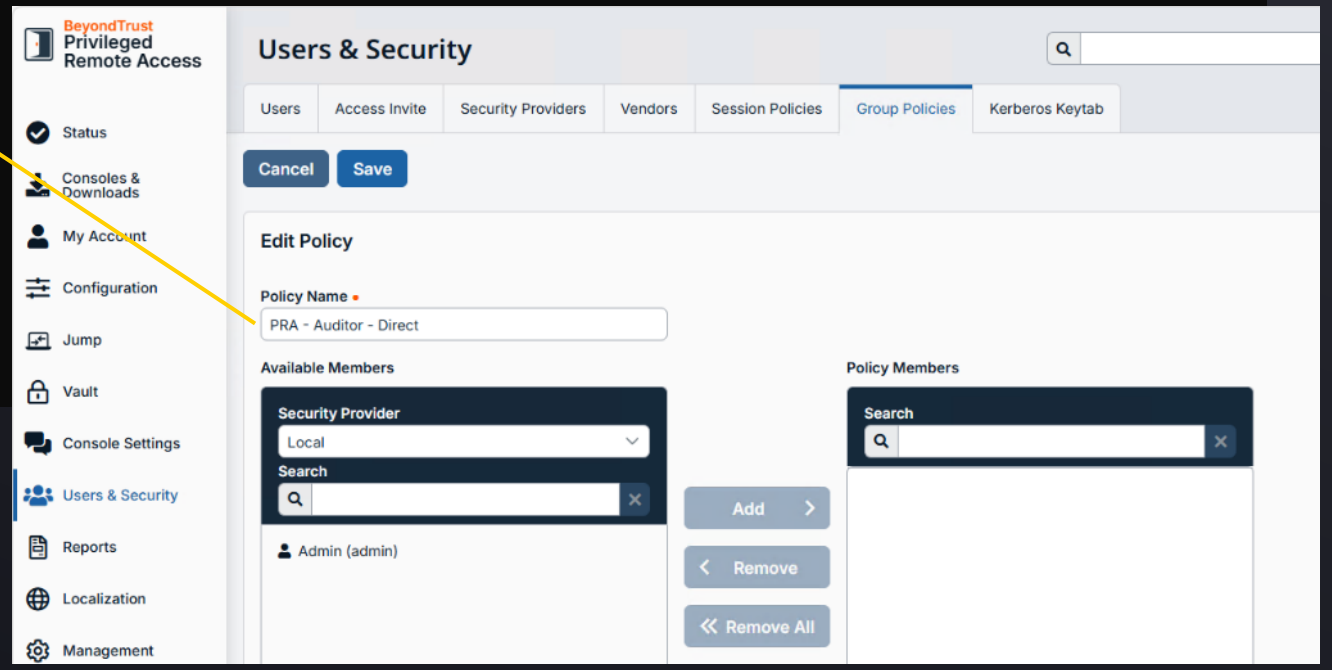


SRA PS Module

Was ist das?

AVANTEC
Competence. Security. Trust.

```
PS C:\Script> Import-Module .\sra-ps\
PS C:\Script> Get-Module

ModuleType Version    PreRelease Name                                ExportedCommands
---------- -------    ---------- ----                                ----------------
Manifest   1.0.1.0               ActiveDirectory                     {Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAccount, Add-ADDomainControllerPass…
Manifest   7.0.0.0               Microsoft.PowerShell.Management     {Add-Content, Clear-Content, Clear-Item, Clear-ItemProperty…}
Manifest   7.0.0.0               Microsoft.PowerShell.Security       {ConvertFrom-SecureString, ConvertTo-SecureString, Get-Acl, Get-AuthenticodeSignature…}
Manifest   7.0.0.0               Microsoft.PowerShell.Utility        {Add-Member, Add-Type, Clear-Variable, Compare-Object…}
Script     2.4.5                 PSReadLine                          {Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PSReadLineKeyHandler, Set-PSReadLi…
Script     0.0.3                 sra-ps                              {Get-EndpointAutomationEndpoint, Get-EndpointAutomationJob, Get-EndpointAutomationJobExecu…

PS C:\Script> Get-GroupPolicy -All

id                                  : 1
name                                : PRA - Auditor - Direct
perm_access_allowed                 : False
access_perm_status                  : not_defined
perm_share_other_team               : False
perm_invite_external_user           : False
perm_session_idle_timeout           : -1
perm_extended_availability_mode_allowed : False
perm_edit_external_key              : False
perm_collaborate                    : False
perm_collaborate_control            : False
perm_jump_client                    : False
```



SRA PS Module

Warum? PowerShell <-> AD Integration

AVANTEC
Competence. Security. Trust.

SRA PS Module

Warum? – Pagination

SRA PS Module

Warum? – Anzahl Zeilen Code

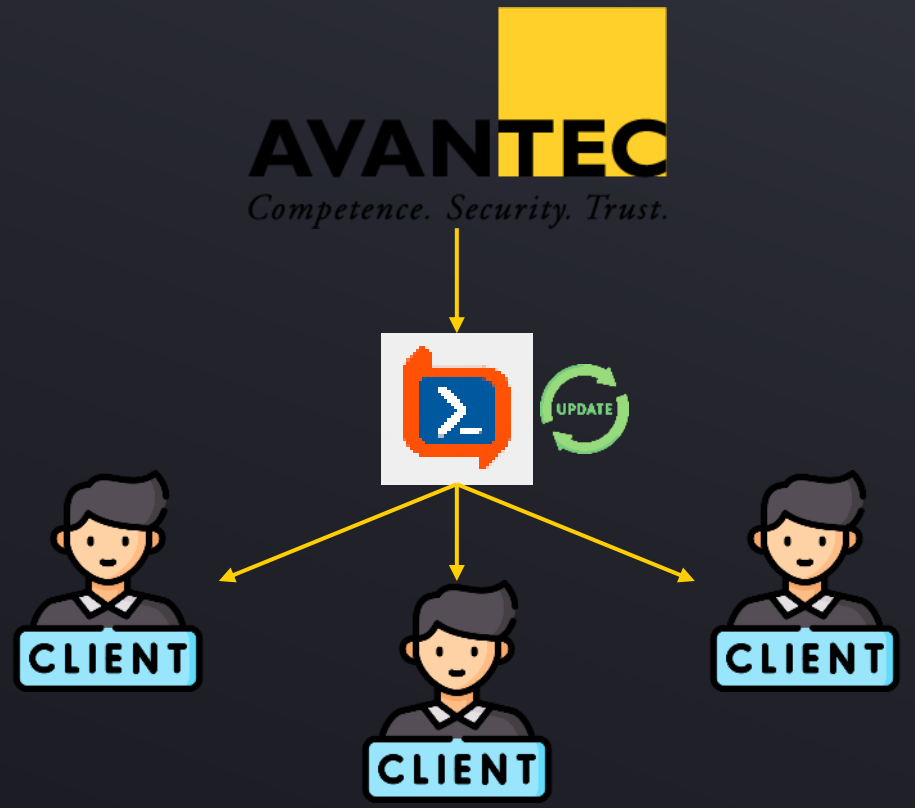
AVANTEC
Competence. Security. Trust.

```powershell
# Get all Group Policies from PRA
$GroupPolicies_PRA_Current_State = @()
#Pagination, get last page for response
$URL = 'https://' + $ApplianceURL + '/api/config/v1/group-policy'
try {
    $AllGPFromPRA = Invoke-WebRequest $URL -Method 'GET' -Headers $headers -UseBasicParsing
} catch {
    $_ | Out-File -FilePath $ErrorLog -Append
}
$LastPage = [int]$AllGPFromPRA.Headers["X-BT-Pagination-Last-Page"][0]

# Get all the Group Policies from PRA and save them in $GroupPolicies_PRA_Current_State
for ($counter = 1; $counter -le $LastPage; $counter++)
{
    $URL = 'https://' + $ApplianceURL + '/api/config/v1/group-policy?per_page=100&current_page=' + $counter + ''
    try {
        $response = Invoke-RestMethod $URL -Method 'GET' -Headers $headers
    } catch {
        $_ | Out-File -FilePath $ErrorLog -Append
        Write-Host "$(Get-Date) Error occurred while retrieving group policies from PRA" -ForegroundColor Red
        "Error occurred while retrieving group policies from PRA" | Out-File -FilePath $ErrorLog -Append
        exit
    }
    $response | ForEach-Object {
        $GroupPolicies_PRA_Current_State += $_
    }
}
```

```
PS C:\Script> Get-GroupPolicy -All

id
name
perm_access_allowed
```

SRA PS Module

Warum? – Hersteller Update



SRA PS Module

Warum? – Verschlüsselung der Secrets

AVANTEC
Competence. Security. Trust.

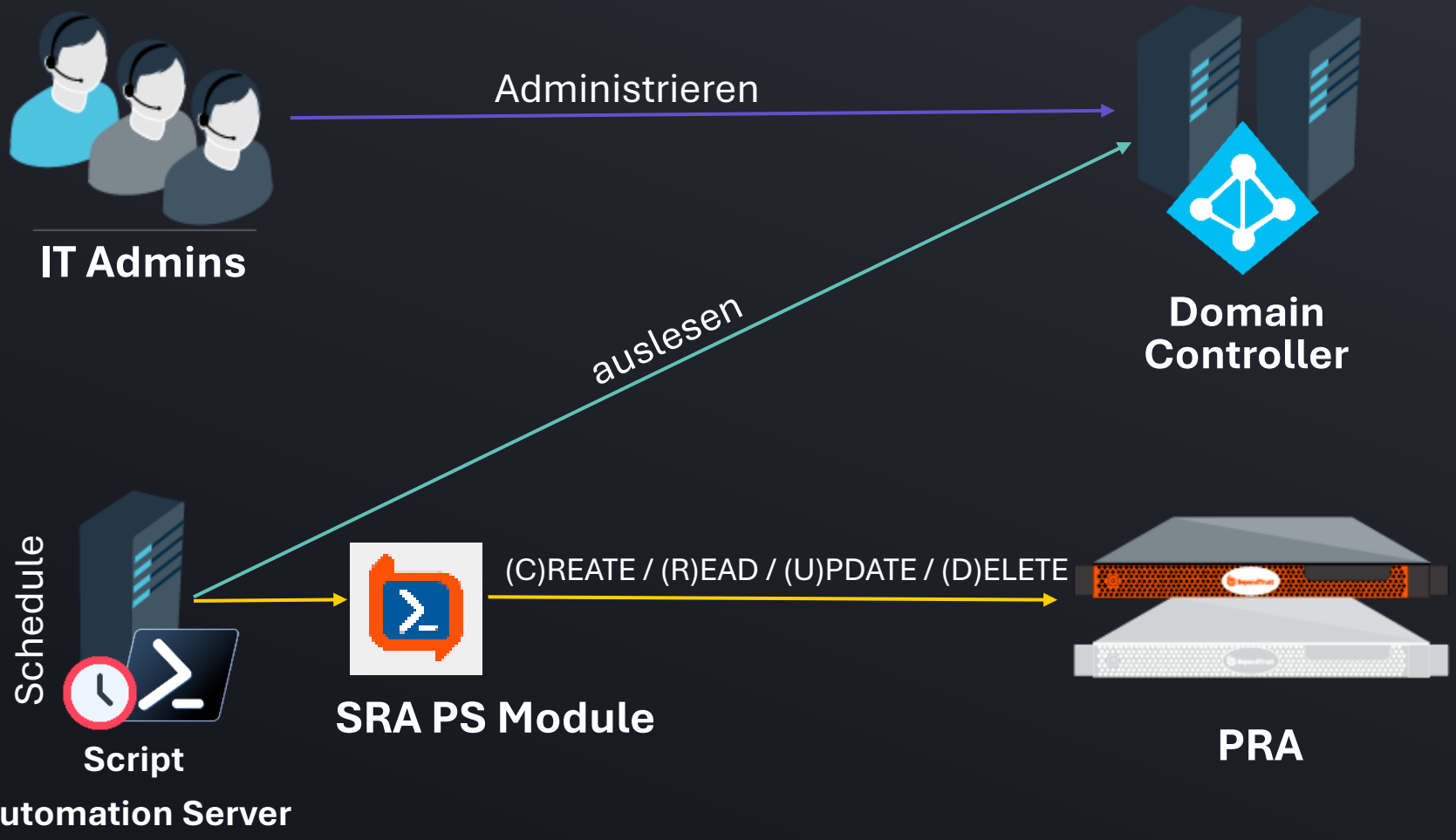
```
$Base64AuthString = [Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("${ClientId}:${ClientSecret}"))

$SecureAuth = ConvertTo-SecureString -String $Base64AuthString
```

sra_api_key.txt - Notepad

File Edit Format View Help

This key can only be used by the user (Administrator) and computer(SCRIPT), which created it was created on. This is the encrypted
key:01000000d08c9ddf0115d1118c7a00c04fc297eb01000000e94ba82b865acf46b3da437b60c50ec000000000020000000000106600000001000020
00000034d955bfc63de2411af96285e006e80e04339b722fe9a87e8bb8c05fe23824bd000000000e8000000002000020000000989af8197d13fe2780f
8d84ecccf7fa6ce3a0e7697f6db19ea8e9840ee75fc5f0000000e0a33f480fbe2e1ae728117d12c9275764f24b73bc7ccae674859c2222048c68f59753
1bbea655aa7d8f6c08905299a40065e14ed8b2439f9bc147de237670a48cf4159b5301d1f166722f0ea10cf596d5040889da843994f39dea0fe0836a28
fa0db63a0b3f5a5b588f3ca8456fda33f2143c34874371acfbf84583fb6dc7d6ed77799ee8bdf7cefad9ace5bfe40f51d9a56c7512de234c14eb69a4b3
bc587e3b232e261aabf87c9cae12421830a29007f6561270255ece8c1bedca545fd6cc3dd2bae9d639650936c3f0209fe5d37d427c50383da620229909
8c6bfea401a5d56ef9adc26631fefa643275fa5434cf400000005e78be574bf1a81ae1303f08c7cd908776a77e520f1c6b7b723fe96781e90394654617
1c37cca1c373248a809eeeaef049fb1805ca830f4c7fba7d01c9e0b52c

Automatisierung mit SRA PS Module

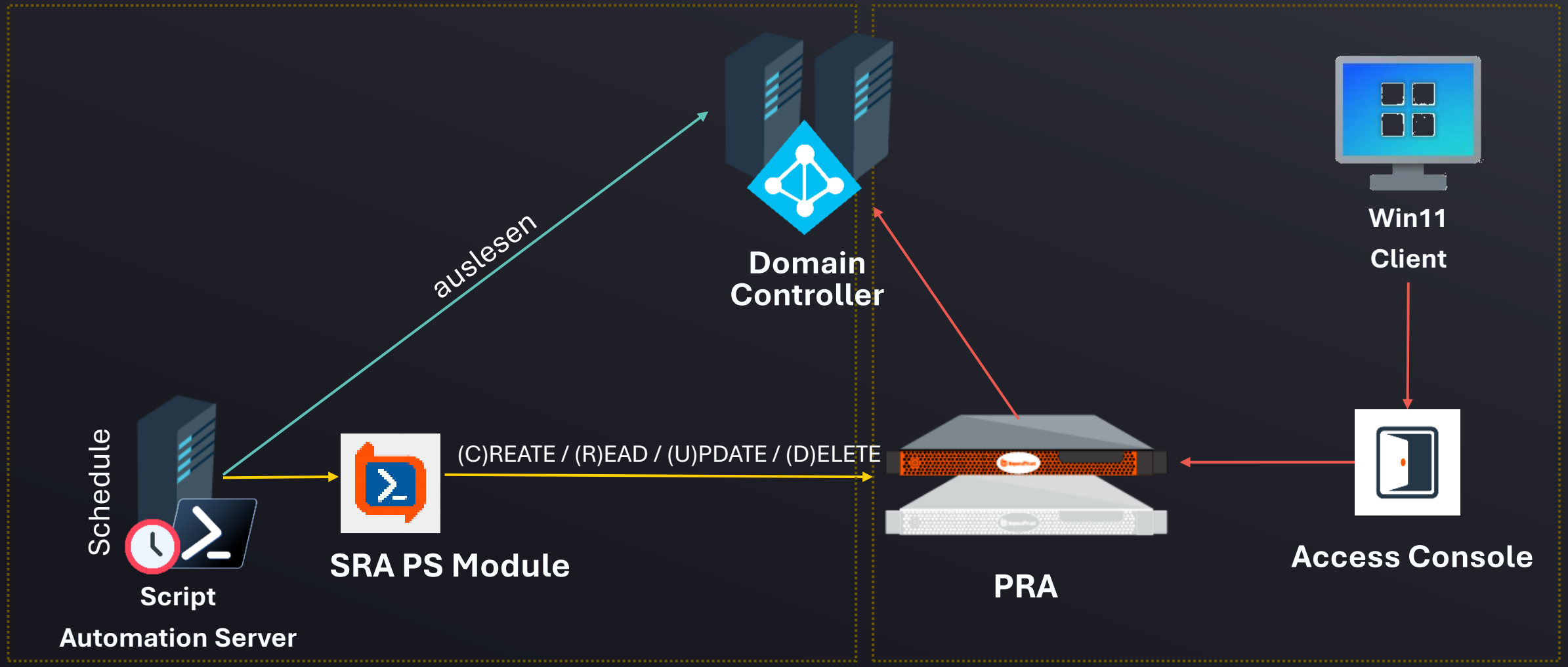


AVANTEC
Competence. Security. Trust.

DEMO

DEMO

Aufbau


auslesen
Domain Controller
Win11 Client
Schedule
(C)REATE / (R)EAD / (U)PDATE / (D)ELETE
Script Automation Server
SRA PS Module
PRA
Access Console

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

viega

Dominic Welsch
IT Team Lead Network & Security
Viega

Viega - TBD

Kunden Case

- TEIL DOMINIC WELSCH

Viega – was wurde automatisiert?

Kunden Case

- Provisionierung von User & Gruppen – SCIM
- Erstellung und Zuweisung von:
  - Endsystemen (Jump Items)
  - Jump Policy & Session Policy
  - Group Policies
- Differenzierung zwischen internen und externen Mitarbeiter
  - Andere Jump & Session Policy

Viega – ein paar Zahlen

Kunden Case

AVANTEC
Competence. Security. Trust.

Was?	EMEA	US	Total
Users	220	30	250
Jump Items / Jump Groups	390	227	617
Group Policies	1506	344	1850

viega

Stand: 05.05.2026

AVANTEC
Competence. Security. Trust.

Q&A

AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.

Nächste Session 13:00

Session 2

Was ist PAM mit Zero Standing Privileges (ZSP)? — Frei, 4. OG

Produkt: BeyondTrust
Referenten: Michael Scherzinger, Jessica Warland

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security — Odermatt, 4. OG

Produkt: zscaler
Referent: Jonas Kugler

Disaster Recovery im Cloud-Zeitalter — Lehmann Steingruber, 5. OG

Produkt: zscaler
Referent: Matthias Geiser

How to secure AI – Ein strategischer Überblick — Cancellara, 4. OG

Produkte: Diverse
Referent: Georg Hegyi