TECH UPDATE
EXPERTENWISSEN FÜR IHRE IT-STRATEGIE

15 JAHRE braincon

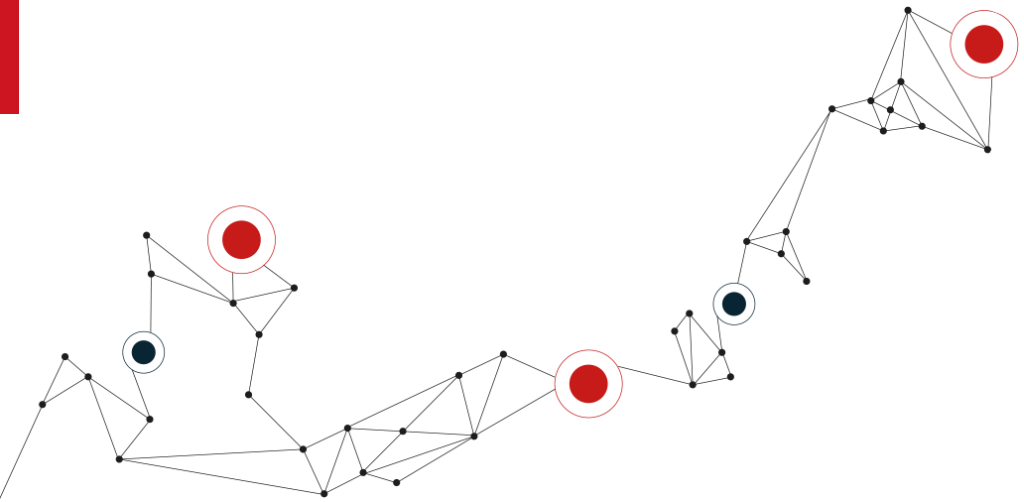
braincon
IT-EXPERTS. NOTHING ELSE.

Von ActiveDirectory-Härtung zu Privileged Access Management (PAM)

Fabio Richter
Senior Solution Expert

Kurzer Überblick

- Recap TechUpdate 2024
  - Bausteine für ein sicheres AD
- Privileged Access Management (PAM)
  - Was sind die Ziele eines PAM-Systems?
  - Wie funktioniert ein PAM-System?
  - Welche Herausforderungen gibt es?
- Wie gehen wir vor?



Recap bcTU2024

Bausteine für ein sicheres AD

Bausteine für ein sicheres AD

Bausteine für ein sicheres AD

Regelmäßige Wartung des AD

- Durchführen von Healthchecks
- Regelmäßiger Reset des krbtgt-Passwortes
- Bereinigen alter Objekte

Bausteine für ein sicheres AD

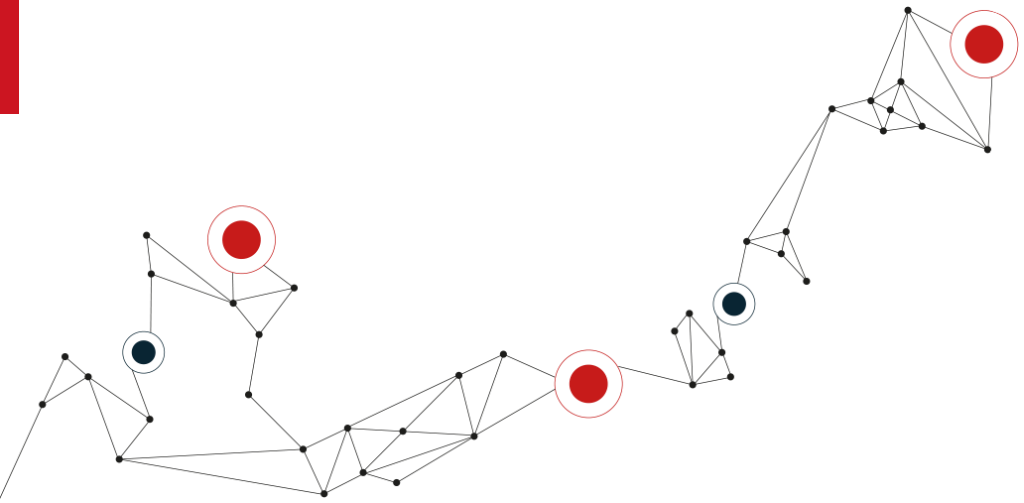
Schließung offener Sicherheits-lücken

- Verbieten alter Protokolle (NTLM, SMBv1, ...)
- Minimierung von administrativen Konten
- Delegationen nach Minimalprinzip erstellen
- Entfernen aller nicht notwendigen SPNs
- Einführung von gMSA-Konten

Bausteine für ein sicheres AD

Etablierung einer Tiering-Struktur

Zugriffe nur über PAWs!

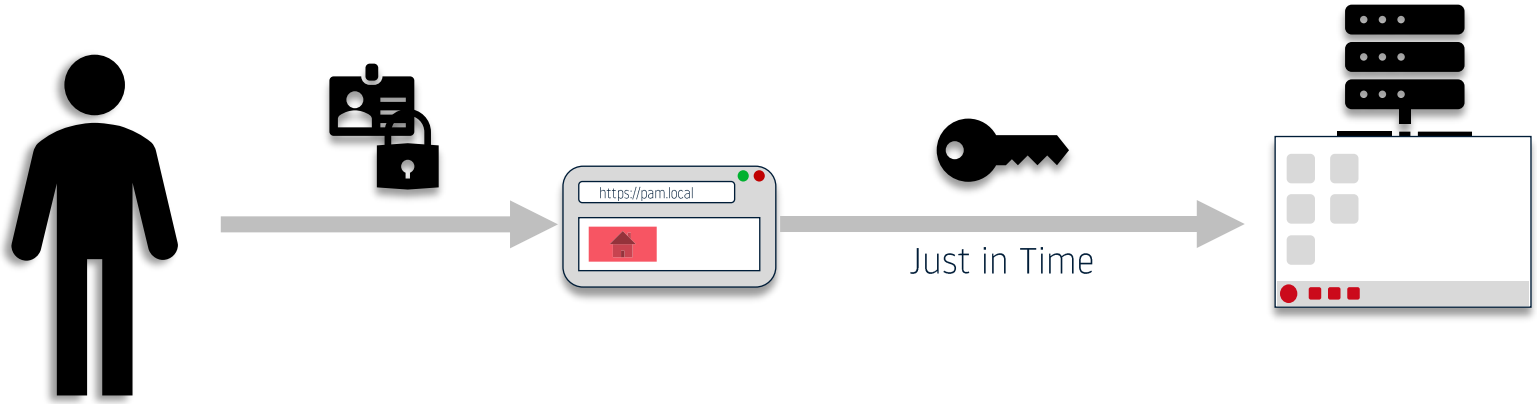


Privileged Access Management

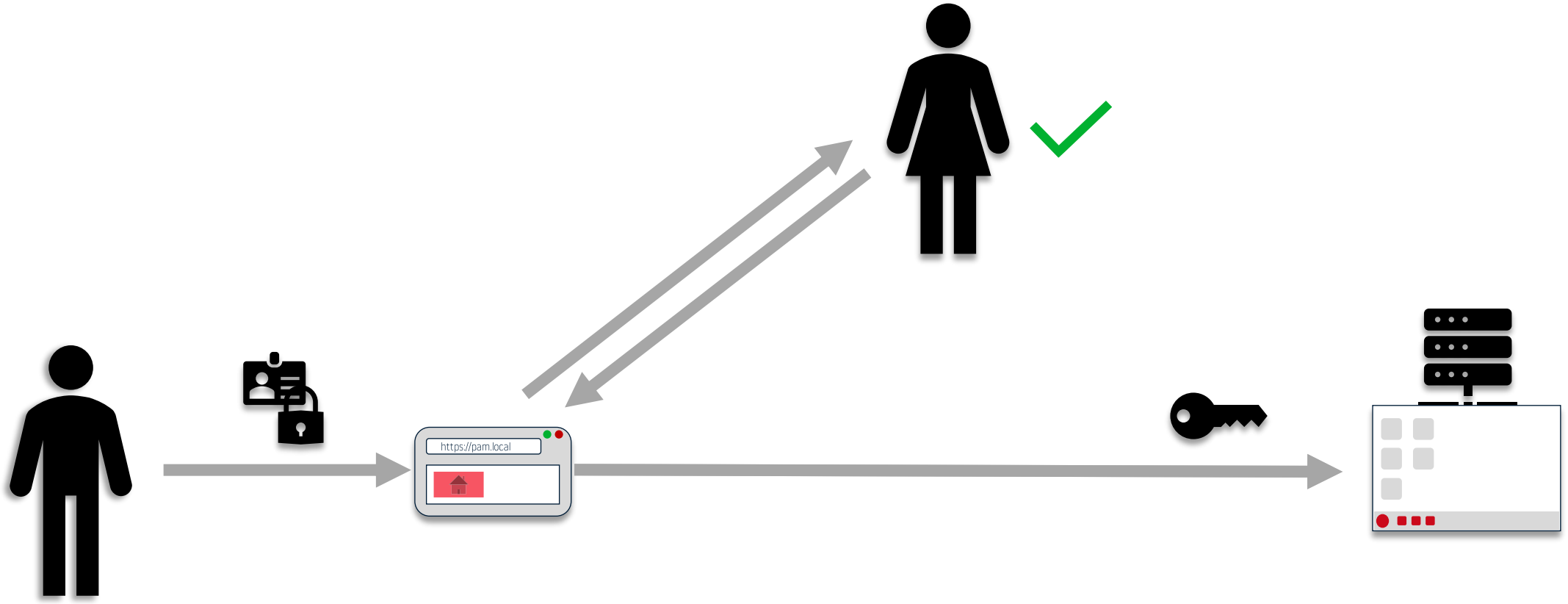
Privileged Access Management - was ist das?

- bietet zentralen Zugriffspunkt zur Administration (im Browser)
- sichert und verwaltet administrative Zugriffe
  - on-Premises MFA
  - Kennwortmanagement und –rotation
  - Just-In-Time- und Just-Enough-Zugriff

Privileged Access Management



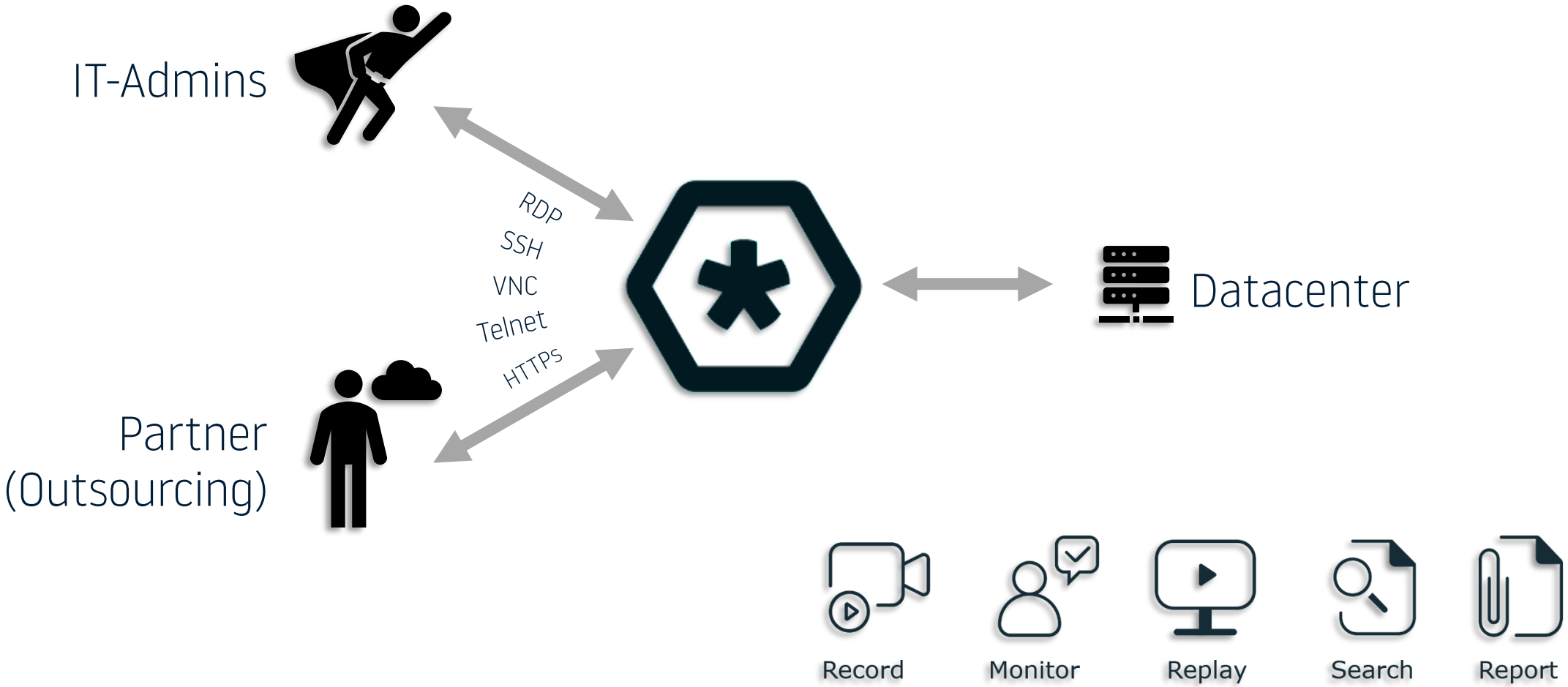
Administrationsprozess mit PAM



Key-Features von PAM

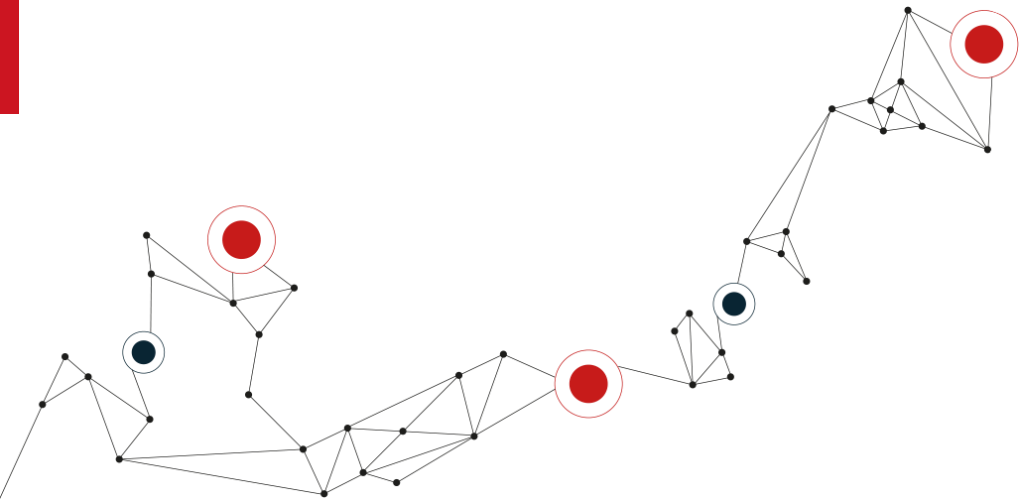
- automatisches Hinzufügen von neuen Systemen durch Anbindung an AD/vCenter
- Kennwortrotation & zentrale Kennwortverwaltung
- Session-Analyse / Anomalie-Check
- OnPrem-MFA für administrative Zugriffe via PAM
  - Microsoft MFA
  - OneLogin App
  - Radius
  - etc.
- Sicherstellung von Compliance-Anforderungen
  - automatisierte Logs
  - Session-Aufzeichnungen
  - Terminieren von Sitzungen
  - Vier-Augen-Prinzip

Safeguard for privileged Sessions – SPS



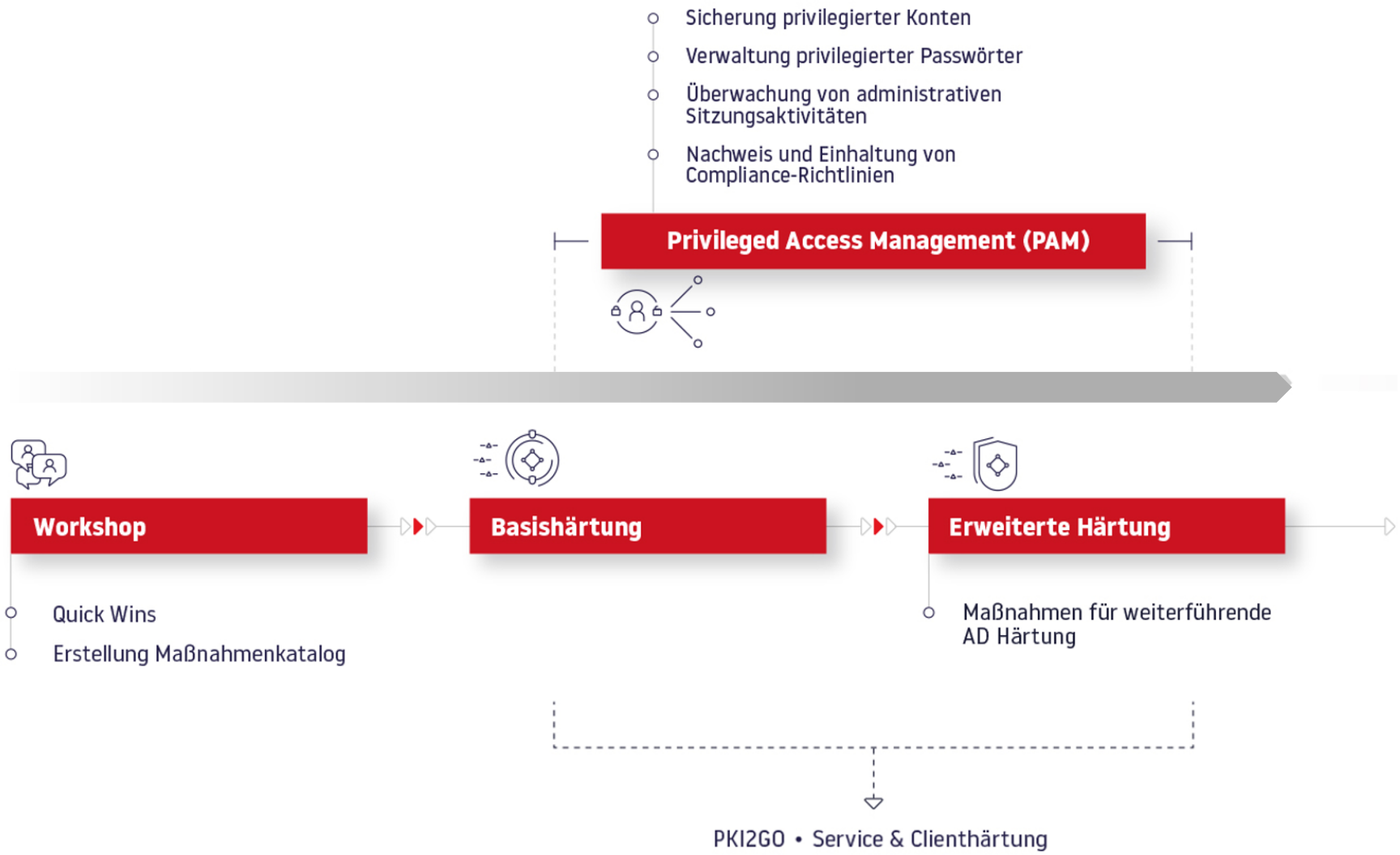
Welche Herausforderungen gibt es?

- Es muss bekannt sein, was auf welchem System läuft.
- Wege zur Administration in Notfällen müssen definiert werden.
- Alle administrativen Verbindungen werden nur aus der PAM-Lösung erlaubt.
- Betriebsrat muss in das Design eingebunden werden.
- Adoption von externen Dienstleistern muss vorab abgestimmt werden.
- Die Einführung muss durch Entscheider gestützt sein.



Wie gehen wir vor?

Wie gehen wir vor?



DANKE

Fragen? Gerne!

braincon
IT-EXPERTS. NOTHING ELSE.

15 JAHRE braincon

braincon GmbH

+49 6071 180 300
info@braincon.de
www.braincon.de

Region Rhein-Main

Altheimer Straße 4
64807 Dieburg

Region Rhein-Ruhr

Lise-Meitner-Straße 1-13
42119 Wuppertal

braincon
IT-EXPERTS. NOTHING ELSE.

15 JAHRE braincon

The Digital Workplace Experts!

Modern. Secured. Managed.