

Identity Health Report — Arvenwerk

Scan: Arvenwerk_20261005_0600 · Report erstellt: 05.10.2026 · Beispielbericht (fiktives Unternehmen)

Beispielbericht. Die Arvenwerk AG ist ein fiktives Unternehmen. Alle Namen, Domänen, Systeme, Konten und Kennzahlen in diesem Bericht sind erfunden und zeigen nur Aufbau und Inhalt eines Identity Health Reports. Der Compliance-Abschnitt zeigt beispielhaft das DORA-Mapping des Toolkits; welche Regelwerke ein Bericht abbildet, wird je Auftrag festgelegt.

RISIKO-SCORE

85 / 100

KRITISCH · 1 kritisch, 3 hoch, 10 Warnungen

REIFEGRAD

2 / 4

Stufe 2 - bereinigt in Teilen, Härtung offen

IDENTIFIZIERTES POTENZIAL

12.495 €/Jahr

davon 9.180 € harte Einsparung

DORA-IAM

16 / 21

PFLICHT offen: 3 mit Befund, 2 ohne Nachweis - Abschnitt 4

NICHT PRÜFBAR

9

Prüfpunkte ohne Datengrundlage — siehe Abschnitt 0

0 · Eingeschränkte Aussagekraft

9 Prüfpunkt(e) konnten nicht erhoben werden. Für diese Punkte trifft der Bericht **keine** Aussage — sie sind weder als in Ordnung noch als auffällig zu lesen. Ursache ist in der Regel ein fehlendes Leserecht oder eine nicht erreichbare Quelle.

Bereich	Prüfung	Ursache	Bedeutung für diesen Bericht
Server	Lokale Gruppen (Erreichbarkeit)	2 von 96 Servern nicht per WinRM lesbar, z.B. AW-LAB-SRV01.arvenwerk.local (WinRM nicht erreichbar/aktiv) AW-OT-HIST02.arvenwerk.local (WinRM nicht erreichbar/aktiv)	Für diese Server liegt KEINE Aussage zu lokalen Gruppen vor (105_LocalGroups_NichtErreichbar.csv).
Server	Anmeldespuren (Profile, Sitzungen)	Kein Server lieferte Profile/Sitzungen (94 ohne WMI-Leserecht, 0 ohne Antwort): Access denied	Tier-0-Anmeldungen auf Nicht-DCs und HasSession-Kanten für Modul 27 fehlen; Scan-Konto braucht lokales Adminrecht (WMI) auf den Servern.
Entra Tenant	Benutzereinstellungen: Entra-Adminportal für Nicht-Admins eingeschränkt, LinkedIn-Kontoverbindungen	Nicht über Microsoft Graph lesbar (nur Entra-Portal: Benutzer > Benutzereinstellungen).	Diese zwei Benutzereinstellungen stehen nicht in 154_.
Entra Authentifizierung	SSPR-Geltungsbereich (für wen aktiviert)	Nicht über Microsoft Graph lesbar (nur Entra-Portal: Kennwortzurücksetzung > Eigenschaften).	Ob SSPR für alle oder eine Gruppe gilt, steht nicht im Bericht; SSPR-Registrierung je Benutzer (153_) ist vollständig.
Entra Apps	Exchange-RBAC-Rollenzuweisungen für Apps (Exchange.ManageAsApp-Rollen)	Nicht über Microsoft Graph lesbar; Prüfung über ExchangeOnlineManagement ist opt-in (Entra.ExoRbacCheck=false).	Welche Exchange-Rollen Apps tragen, steht nicht im Bericht (167_).
Domain Controller	DC-Probe: Patchstand, WebClient/Spooler-Dienst, DSRM-Anmeldung	Posture.DcProbe = false (Standard): kein CIM/WinRM-Zugriff auf DCs.	S-DC-NotUpdated, A-DC-WebClient, P-RecoveryModeUnprotected, MS14-068/MS17-010 nur über die opt-in-Probe prüfbar (197_DC_Probe.csv).
Domain Controller	Netzproben: LDAPS-Protokollversionen, SMB-Signierung am DC	Posture.NetworkProbes = false (Standard): keine TLS-/SMB-Handshakes zu DCs.	A-DCLdapsProtocol/-Advanced und die tatsächliche SMB-Signierungsanforderung nur über die opt-in-Probe prüfbar (192_DC_Netzproben.csv); GPO-Sicht in 180_/181_.

Bereich	Prüfung	Ursache	Bedeutung für diesen Bericht
Domain Controller	NTLM-/Trust-Nutzung aus DC-Ereignisprotokollen	Posture.EventLogProbe = false (Standard): kein Zugriff auf die Ereignisprotokolle der DCs.	Wie stark NTLM noch genutzt wird (Grundlage der NTLM-Abschaltung), ist nur über die opt-in-Probe messbar (197_DC_Ereignisse.csv).
AD CS	ESC8: Web-Enrollment (certsrv) über HTTP	Posture.CaProbe = false (Standard): keine HTTP-Anfrage an die CA-Hosts.	Ob certsrv über HTTP erreichbar ist (NTLM-Relay-Ziel, A-CertEnrollHttp), steht nicht im Bericht; CES-Endpunkte aus dem AD (85_, Spalte CesEndpunkte) sind gelesen.

1 · Executive Summary

Wichtigste Befunde (4 von 4 kritischen und hohen Befunden; alle kritischen enthalten, vollständige Liste in Abschnitt 3):

- **[DORA-IAM]** DORA / RTS (EU) 2024/1774 - Identitäts- und Zugangsmanagement (mit BAIT-Querverweis): 5 PFLICHT-Regeln offen (3 mit Befund, 0 nicht prüfbar, 2 nicht abgedeckt) - Abschnitt 4
- **[KRITISCH]** Veröffentlichte Zertifikatvorlagen mit vollständigem Eskalationspfad (ESC1: Antragsteller bestimmt Identität + Anmelde-EKU + keine Genehmigung + breite Registrierung; ESC2/ESC3: Sub-CA bzw. Registrierungsstelle breit registrierbar) — 1 (davon ESC1: 1)
- **[HOCH]** Exponierte Relay-/Coerce-Kanäle (NTLM-Relay) — 3 Kanäle
- **[HOCH]** Aktive Tier-0-Konten nicht in "Protected Users" — 7
- **[HOCH]** DORA / RTS (EU) 2024/1774 - Identitäts- und Zugangsmanagement (mit BAIT-Querverweis): PFLICHT-Regeln mit Befund — 3 von 21

Sofortmaßnahmen (scriptgestützt in wenigen Tagen umsetzbar; nach Schweregrad, 10 von 10):

- **Veröffentlichte Zertifikatvorlagen mit vollständigem Eskalationspfad (ESC1: Antragsteller bestimmt Identität + Anmelde-EKU + keine Genehmigung + breite Registrierung; ESC2/ESC3: Sub-CA bzw. Registrierungsstelle breit registrierbar)** (1 (davon ESC1: 1)) — Sofort entschärfen: Genehmigungspflicht aktivieren, „Antragsteller liefert Subject“ abschalten oder Registrierungsrechte begrenzen (87_-Datei, Spalte Befunde).
- **Aktive Tier-0-Konten nicht in "Protected Users"** (7) — In Wellen aufnehmen (kein NTLM, kein RC4, keine Delegation, 4-h-TGT) — Betriebskonten vorher testen (75_-Datei, Spalte InProtectedUsers = False; PingCastle P-ProtectedUsers).
- **Aktivierte Konten ohne Anmeldung (AD UND Entra, effektiv inaktiv)** (64) — Freigabeprozess starten (Modul 2), dann staged deaktivieren (Modul 3).
- **Lizenzierte, aber effektiv inaktive Konten** (23) — Lizenz-Reclaim sofort möglich (Quick Fix) - siehe Wertrechner.
- **Leere Gruppen** (61) — Nach Prüfung löschen (Quick Fix).
- **Wirkungslose GPOs (leer / unverlinkt / deaktiviert / leeres Filtering)** (12 von 84) — Nach Sichtung entfernen - reine Verwaltungslast (siehe Wertrechner).
- **Abgelaufene App-Anmeldeinformationen** (14) — 14 abgelaufene Secrets/Zertifikate (Hygiene/Betriebsrisiko).
- **Inaktive Gastkonten** (142) — 142 aktivierte Gastkonten ohne Anmeldung seit >90 Tagen (oder nie).
- **Inaktive Geräteobjekte** (96) — 96 aktivierte Geräte ohne Aktivität seit > 180 Tagen. Veraltete Geräteobjekte erfüllen CA-Gerätebedingungen weiter und verfälschen Compliance-Zahlen - deaktivieren, nach 30 Tagen löschen (170_Entra_Geraete.csv).
- **Anwendungen ohne Anmeldung (Bereinigung)** (37) — 37 eigene/Drittanbieter-Anwendungen ohne Anmeldung seit > 180 Tagen - Bereinigungskandidaten (160_-Datei).

Kennzahlen im Überblick

Ist-Werte dieses Laufs, Trend zum Vorlauf Arvenwerk_20260907_0600. Keine Konten, keine Beträge, keine Sollwerte — der Abgleich gegen Zielwerte gehört dem Projekt (230_Kennzahlen.csv liefert alle 1162 Kennzahlen mit stabilen Schlüssel(n). 1 Zeile(n) nicht erhoben: Modul nicht gelaufen oder Bereich nicht lesbar.

Kennzahl	Ist	Trend	Quelle
Lokale Adminrechte (Server)			
Personen direkt in lokalen Admin-Gruppen	0	↓ -3 (besser)	101_
Server mit Personen direkt in Admin-Gruppen	0	↓ -2 (besser)	101_
Gleichnamige lokale Adminkonten auf 3+ Servern	0	→ unverändert	103_
Aktive lokale Adminkonten (neben RID 500)	0	→ unverändert	103_
Server gelesen / nicht erreichbar	94 / 2	↑ +1 (besser)	106_
Tier 0			
Tier-0-Konten gesamt	14	→ unverändert	75_
Tier-0-Konten delegierbar	0	→ unverändert	75_
Tier-0-Konten nicht in Protected Users	7	↓ -2 (besser)	75_
Tier-0-Konten mit Postfach	0	→ unverändert	62_
Effektives Tier 0 jenseits Well-Known: unerklärt	0	→ unverändert	61_
Nicht erwartete Replikationsrechte (DCSync-ACEs)	0	→ unverändert	66_
Konten mit Tier-Bruch (Tier 0 + Tier 1)	0	→ unverändert	232_
Gruppen mit Wirkung in mehreren Tiers	0	→ unverändert	232_
Server mit Tier-0-Prinzipal in lokalen Administratoren	0	↓ -1 (besser)	231_
Tier-0-Konten synchronisiert nach Entra	0	→ unverändert	238_
Adminkonten ohne zuordenbare Person	0	→ unverändert	239_
Personen mit mehreren Konten gleicher Wirkung	0	→ unverändert	239_
Delegation und GPO			
Hochrisiko-Delegationen (OU-ACLs)	9	→ unverändert	64_
Gefährliche erweiterte Rechte außerhalb Tier 0	0	→ unverändert	136_
Wirkungslose GPOs	12	↓ -3 (besser)	72_
Härtungsabdeckung Ø (%)	91	↑ +3 (besser)	181_
Struktur und Altlasten			
Sync-Abweichungen je Konto (Scope/Kennzeichen/Entra)	0	→ unverändert	48_
Aktivierte Konten in Quarantäne-OU, weiter synchronisiert	0	→ unverändert	48_
Benutzer im Standardcontainer CN=Users	3	→ unverändert	10_
Computer im Standardcontainer CN=Computers	0	→ unverändert	20_
Objekte mit SIDHistory	0	→ unverändert	19_
SIDHistory-Einträge aus unbekannten Domänen	0	→ unverändert	19_
Dienstkonten unter Mindest-Kennwortlänge	0	→ unverändert	16_
OUs mit Server und Clients gemischt	1	→ unverändert	235_
Objekte in Quarantäne über Löschfrist	0	→ unverändert	236_
Aktivierte Konten in Quarantäne-OUs	0	→ unverändert	236_
Verschobene Objekte mit verlorenen GPO-Einstellungen	0	→ unverändert	237_
Computer mit LAPS-Kennwort (ohne DCs)	1.203 / 1.210	↑ +7 (besser)	241_

Kennzahl	Ist	Trend	Quelle
Computer mit abgelaufenem LAPS-Kennwort	0	→ unverändert	241_
Fähige Computer ohne LAPS (aktiv)	0	→ unverändert	241_
Dienstkonten unter Domänen-Kennwortrichtlinie	0	→ unverändert	15b_
Exchange-Server im AD registriert	0	→ unverändert	243_
Aktive Server ohne Support (EOL)	0	→ unverändert	25_
ESC1-Vorlagen veröffentlicht	1	→ unverändert	87_
Entra ID			
Permanente Rollenzuweisungen (aktiv)	18	↓ -3 (besser)	150_
Eligible Rollenzuweisungen (PIM)	25	↑ +3	150_
Break-Glass-Kandidaten	2	→ unverändert	242_
Cloud-Adminkonten (Rolleninhaber)	19	→ unverändert	242_
Cloud-Adminkonten synchronisiert aus AD	0	→ unverändert	242_
Tier-0-Rollen: permanente Zuweisung erlaubt (PIM)	0	→ unverändert	150_
CA-Richtlinien ohne Break-Glass-Ausschluss	0	→ unverändert	152_
CA-Richtlinien Report-only über Schwelle	0	→ unverändert	152_
Benutzer im CA-Scope ohne P1-Serviceplan	0	→ unverändert	158_
Aktive Mitglieder ohne MFA-Methode	0	→ unverändert	153_
Tier-0-Apps ohne Besitzer	0	→ unverändert	163_
Apps nur mit Client Secret (ohne Microsoft)	9	↓ -2 (besser)	165_
App-Entscheidungen offen (Apps.Decisions)	0	→ unverändert	166_
Benutzer direkt in Administratoren per Intune	0	→ unverändert	233_
Autopilot-Profil mit Benutzertyp Administrator	0	→ unverändert	234_
Gäste ohne Sponsor (aktiviert)	38	↓ -3 (besser)	84_
Mitglieder ohne MFA-Methode	0	→ unverändert	153_
Admins ohne phishing-resistente Methode	0	→ unverändert	153_
Inaktive Gäste (aktiviert, ohne Anmeldung)	142	↓ -6 (besser)	84_
Lizenzierte inaktive Konten	23	↓ -2 (besser)	40_
Inaktive Geräte	96	↑ +5 (schlechter)	171_
Angriffspfade			
Aktive Benutzer mit Pfad zu Tier 0	0	→ unverändert	212_
Kerberoastbare Konten mit Pfad zu Domain Admins	0	→ unverändert	213_
Systeme mit unbeschränkter Delegation (Ziel)	0	→ unverändert	217_
Exponierte Relay-/Coerce-Kanäle	3 / 12	→ unverändert	218_
Sperrpunkte (Chokepoints) identifiziert	0	→ unverändert	214_
Entra: Kontrollpfade			
Entra-Benutzer mit Pfad zu Tier 0	0	→ unverändert	219_
AD-Tier-0-Konten synchronisiert (hybrid)	0	→ unverändert	219_
Synchronisierte Besitzer von Entra-Objekten	0	→ unverändert	219_
Struktur und Altlasten			
SIDHistory gefahrlos bereinigbar (Quick-Win)	0	→ unverändert	19a_
SIDHistory-Einträge mit Risiko HOCH (Gruppen)	0	→ unverändert	19a_
SIDHistory unbekannte Domänen mit Hypothese	0	→ unverändert	19b_

Kennzahl	Ist	Trend	Quelle
Delegation und GPO			
GPOs durch breite Prinzipale bearbeitbar	0	→ unverändert	77_
GPO macht breite Prinzipale zu lokalen Admins	0	→ unverändert	128_
Struktur und Altlasten			
DNS-Zonen mit unsicheren dynamischen Updates	0	→ unverändert	196_
CA-Zertifikate mit schwachem Schlüssel	0	→ unverändert	195_
Server: lokale Gruppen			
Tier-0-Anmeldespuren auf Nicht-Tier-0-Systemen	nicht erhoben		110_
Entra ID			
Secure Score	318 / 373	↑ +6 (besser)	157_

Entwicklung seit letztem Scan

Vergleich mit: Arvenwerk_20260907_0600 · 19 Kennzahlen verbessert, 1 verschlechtert. Details: Drift-CSV im Scan-Ordner.

Kennzahl	Vorher	Jetzt	Δ	Bewertung
Aktivierte Benutzerkonten	1.506	1.512	↑ +6	Veränderung
Effektiv inaktive Konten	70	64	↓ -6	verbessert
Lizenzierte inaktive Konten	25	23	↓ -2	verbessert
UPN-Befunde	0	0	→ 0	unverändert
Sync-Lücken (AD ohne Entra)	0	0	→ 0	unverändert
Leere Gruppen	73	61	↓ -12	verbessert
Zirkelverschachtelungen	0	0	→ 0	unverändert
User über Token-Warnschwelle	0	0	→ 0	unverändert
Effektiv privilegierte User	6	6	→ 0	unverändert
Hochrisiko-Delegationen	9	9	→ 0	unverändert
Hochrisiko-Delegationen ungeklärt	0	0	→ 0	unverändert
Wirkungslose GPOs	15	12	↓ -3	verbessert
Kritische Zertifikatvorlagen	1	1	→ 0	unverändert
Vorlagen mit Schreibrechten	0	0	→ 0	unverändert
SYSVOL-Dateien mit Kennwort	0	0	→ 0	unverändert
AdminSDHolder-Abweichungen	0	0	→ 0	unverändert
Kennwörter in Beschreibungsfeldern	0	0	→ 0	unverändert
Trusts ohne selektive Authentifizierung	0	0	→ 0	unverändert
Trusts ohne SID-Filterung	0	0	→ 0	unverändert
Schlüsselanmeldeinformationen verdächtig	0	0	→ 0	unverändert
DC-Objekte mit falschem Besitzer	0	0	→ 0	unverändert
Tier-0-Konten ohne Delegationsschutz	0	0	→ 0	unverändert
Überalterte Maschinenkennwörter (aktiv)	0	0	→ 0	unverändert
Dienstkonten mit weiter Streuung	0	0	→ 0	unverändert
Verwaltete Dienstkonten (gMSA)	6	7	↑ +1	verbessert
Fehlende Härtungsthemen	0	0	→ 0	unverändert
Exponierte Angriffstechniken	1	1	→ 0	unverändert
Dienstkonten mit SPN (privilegiert)	0	0	→ 0	unverändert
SPN-Konten ohne AES	0	0	→ 0	unverändert
Unerwartete Replikationsrechte	0	0	→ 0	unverändert
EOL-Server aktiv (ohne Support)	0	0	→ 0	unverändert
EOL-Computerobjekte inaktiv (Server)	0	0	→ 0	unverändert
EOL-Clients	0	0	→ 0	unverändert
SIDHistory aus unbekannten Domänen	0	0	→ 0	unverändert
Unbeschränkte Delegation (Nicht-DC)	0	0	→ 0	unverändert
BSI-Verstöße Service-Passwortlänge	0	0	→ 0	unverändert
Personenkonten Passwort läuft nie ab	0	0	→ 0	unverändert
AS-REP-angreifbare Konten	0	0	→ 0	unverändert
Konten ohne AES	0	0	→ 0	unverändert

Kennzahl	Vorher	Jetzt	Δ	Bewertung
krbtgt-Passwortalter (Tage)	35	63	↑ +28	Veränderung
SIDHistory-Benutzer (bis v3.2.0: alle Objekte)	0	0	→ 0	unverändert
Benutzer ohne Kennwortpflicht (PASSWD_NOTREQD)	0	0	→ 0	unverändert
Benutzer mit reversiblen Kennwort	0	0	→ 0	unverändert
Benutzer mit Kerberos-DES	0	0	→ 0	unverändert
SIDHistory eigene Domäne	0	0	→ 0	unverändert
Delegationen mit Ziel DC	0	0	→ 0	unverändert
SIDHistory-Objekte gesamt	0	0	→ 0	unverändert
SIDHistory-Einträge gesamt	0	0	→ 0	unverändert
SIDHistory-Einträge unbekannte Domänen	0	0	→ 0	unverändert
SIDHistory-Gruppen	0	0	→ 0	unverändert
Fremd-SIDs in privilegierten Gruppen	0	0	→ 0	unverändert
Alt-SIDs mit Rechten (SIDHistory-Domänen)	0	0	→ 0	unverändert
Verwaiste SIDs eigene Domäne (ACLs, lokale Gruppen)	0	0	→ 0	unverändert
Fremde SIDs ohne Trust-/SIDHistory-Bezug	0	0	→ 0	unverändert
Effektives Tier 0 unerklärt	0	0	→ 0	unverändert
Erwartete Sync-Konten mit DCSync	1	1	→ 0	unverändert
Konten mit Tier-Bruch (232_)	0	0	→ 0	unverändert
Gruppen mit Wirkung in mehreren Tiers	0	0	→ 0	unverändert
Personen direkt in lokalen Admin-Gruppen	3	0	↓ -3	verbessert
Server mit Tier-0-Prinzipal in Administratoren (231_)	1	0	↓ -1	verbessert
Sync-Abweichungen je Konto (48_)	0	0	→ 0	unverändert
Aktivierte Konten in Quarantäne-OU, synchronisiert	0	0	→ 0	unverändert
Tier-0-Konten synchronisiert (238_)	0	0	→ 0	unverändert
Adminkonten ohne Personenzuordnung	0	0	→ 0	unverändert
Entra: Cloud-Adminkonten synchronisiert	0	0	→ 0	unverändert
Entra: Tier-0-Rollen permanent erlaubt (PIM)	0	0	→ 0	unverändert
Entra: CA Report-only über Schwelle	0	0	→ 0	unverändert
Entra: aktive Mitglieder ohne MFA	0	0	→ 0	unverändert
Entra: Benutzer im CA-Scope ohne P1	0	0	→ 0	unverändert
Gleichnamige lokale Adminkonten (3+ Server)	0	0	→ 0	unverändert
Benutzer im Standardcontainer	3	3	→ 0	unverändert
Computer im Standardcontainer	0	0	→ 0	unverändert
Härtungsabdeckung Ø (%)	88	91	↑ +3	verbessert
ESC1-Vorlagen veröffentlicht	1	1	→ 0	unverändert
Entra: Tier-0-Apps ohne Besitzer	0	0	→ 0	unverändert
Entra: inaktive Gäste	148	142	↓ -6	verbessert
Entra: lizenzierte inaktive Konten	25	23	↓ -2	verbessert
Entra: inaktive Geräte	91	96	↑ +5	verschlechtert
Entra: Secure Score	312	318	↑ +6	verbessert
Tier-0-Konten deaktiviert	1	0	↓ -1	verbessert
Tier-0-Konten inaktiv (aktiviert)	0	0	→ 0	unverändert

Kennzahl	Vorher	Jetzt	Δ	Bewertung
Tier-0-Konten Kennwort nie ablaufend	0	0	→ 0	unverändert
Tier-0-Konten nicht in Protected Users	9	7	↓ -2	verbessert
DC-Maschinenkennwörter > 45 Tage	0	0	→ 0	unverändert
Prinzipale nur RC4/DES	0	0	→ 0	unverändert
Gefährliche erweiterte Rechte	0	0	→ 0	unverändert
Kritische Rechte für breite Gruppen	0	0	→ 0	unverändert
Trusts ohne AES	0	0	→ 0	unverändert
Inaktive Domain Controller	0	0	→ 0	unverändert
Schema Admins Mitglieder	0	0	→ 0	unverändert
Operator-Gruppen Mitglieder	0	0	→ 0	unverändert
Entra: Gäste mit Tier-0-Rolle	0	0	→ 0	unverändert
Entra: deaktivierte Tier-0-Prinzipale	1	0	↓ -1	verbessert
Entra: Geräte mit EOL-OS (aktiv)	0	0	→ 0	unverändert
OUs mit Server und Clients gemischt (235_)	1	1	→ 0	unverändert
Objekte in Quarantäne über Löschfrist (236_)	0	0	→ 0	unverändert
Aktivierte Konten in Quarantäne-OUs	0	0	→ 0	unverändert
Verschobene Objekte mit GPO-Verlust (237_)	0	0	→ 0	unverändert
Computer mit Windows-LAPS-Kennwort (241_)	1.196	1.203	↑ +7	verbessert
Computer mit abgelaufenem LAPS-Kennwort	0	0	→ 0	unverändert
Fähige Computer ohne LAPS (aktiv)	0	0	→ 0	unverändert
Dienstkonten unter Domänen-Kennwortrichtlinie (15b_)	0	0	→ 0	unverändert
Dienstkonten unter Mindestlänge (Password.ServiceAccountMinLength)	0	0	→ 0	unverändert
Exchange-Server im AD registriert (243_)	0	0	→ 0	unverändert
Exchange-Server ohne Support	0	0	→ 0	unverändert
Entra: Apps nur mit Client Secret	11	9	↓ -2	verbessert
Entra: abgelaufene App-Credentials (165_)	17	14	↓ -3	verbessert
Entra: App-Entscheidungen offen (166_)	0	0	→ 0	unverändert
Entra: Benutzer direkt in Administratoren per Intune (233_)	0	0	→ 0	unverändert
Entra: Autopilot-Profile mit Benutzertyp Administrator (234_)	0	0	→ 0	unverändert
Entra: Gäste ohne Sponsor	41	38	↓ -3	verbessert
Entra: Lizenzen gruppenbasiert (%)	94	97	↑ +3	verbessert
Aktive Benutzer mit Pfad zu Tier 0 (212_)	0	0	→ 0	unverändert
Kerberoastbare mit Pfad zu Domain Admins	0	0	→ 0	unverändert
Exponierte Relay-/Coerce-Kanäle (218_)	3	3	→ 0	unverändert
Entra-Benutzer mit Pfad zu Tier 0 (219_)	0	0	→ 0	unverändert
AD-Tier-0-Konten synchronisiert (hybrid)	0	0	→ 0	unverändert
SIDHistory gefahrlos bereinigbar (Quick-Win)	0	0	→ 0	unverändert
SIDHistory-Einträge Risiko HOCH (Gruppen)	0	0	→ 0	unverändert
GPOs durch breite Prinzipale bearbeitbar (77_)	0	0	→ 0	unverändert
GPO macht breite Prinzipale zu lokalen Admins (128_)	0	0	→ 0	unverändert
DNS-Zonen mit unsicheren Updates (196_)	0	0	→ 0	unverändert
CA-Zertifikate mit schwachem Schlüssel (195_)	0	0	→ 0	unverändert

Kennzahl	Vorher	Jetzt	Δ	Bewertung
Besitzer von Tier-0-Rollengruppen ohne Rolle (155_)	0	0	→ 0	unverändert

Entra-Rollen: Zuweisungsart je Rolle

Rollen, deren permanente oder eligible Zuweisungen sich seit dem Vorlauf geändert haben (150_Entra_Rollen_Uebersicht.csv). Umzug permanent → eligible ist das Zielbild von PIM.

Rolle	Permanent	Eligible	Bewertung
Global Administrator (Tier 0)	3 → 2	3 → 4	permanent → eligible
Privileged Role Administrator (Tier 0)	1 → 0	1 → 2	permanent → eligible
Exchange Administrator (Tier 0)	2 → 1	1 → 2	permanent → eligible

2 · Wertrechner

Alle Werte konservativ gerechnet, Formeln und Annahmen offen. Harte Einsparungen sind kassenwirksam; Betriebsaufwand wird bei Umsetzung frei.

Art	Befund	Formel	Annahme	€ / Jahr
Harte Einsparung	Lizenzen auf effektiv inaktiven Konten	31 Lizenzzuweisungen × SKU-Preis × 12 Monate	Preisliste It. Config abzüglich 30 % Kundenrabatt; unbekannte SKU = 15 €/Monat	9.180 €
Betriebsaufwand	Pflege wirkungsloser GPOs	12 GPOs × 3 h/Jahr × 85 €/h	Konservativ: Test-, Doku- und Troubleshooting-Aufwand je GPO	3.060 €
Betriebsaufwand	Review/Rezertifizierung privilegierter Zugriffe	6 privilegierte User × 30 min/Jahr × 85 €/h	Nur der Review-Aufwand; Reduktion der Anzahl senkt ihn direkt	255 €
Summe				12.495 €

3 · Befunde im Detail

● Angriffspfade

Bewertung	Befund	Messwert	Empfehlung
HOCH	Exponierte Relay-/Coerce-Kanäle (NTLM-Relay)	3 Kanäle	Relay-Ziele härten: SMB-/LDAP-Signierung erzwingen, LDAP Channel Binding, EPA für Web-Enrollment, WebClient/Spooler auf DCs aus (218_Relay_Exposition.csv). Ist-Bewertung aus Härtingsregeln, keine aktive Netzprobe. LDAP (Domain Controller) Coerce: MS-RPRN (Spooler) NTLM (Domain Controller)

● Zertifikatsdienste (PKI)

Bewertung	Befund	Messwert	Empfehlung
KRITISCH	Veröffentlichte Zertifikatvorlagen mit vollständigem Eskalationspfad (ESC1: Antragsteller bestimmt Identität + Anmelde-EKU + keine Genehmigung + breite Registrierung; ESC2/ESC3: Sub-CA bzw. Registrierungsstelle breit registrierbar) QF	1 (davon ESC1: 1)	Sofort entschärfen: Genehmigungspflicht aktivieren, „Antragsteller liefert Subject“ abschalten oder Registrierungsrechte begrenzen (87_-Datei, Spalte Befunde).
INFO	Zertifizierungsstellen im Einsatz	1 CA(s), 27 Vorlagen	Prüfaufträge beachten: CA-Flag für SAN-Übernahme, Web-Registrierung/NDES als Relay-Ziel, CA-Auditing (88_-Datei).

● Angriffsflächen

Bewertung	Befund	Messwert	Empfehlung
INFO	Erwartete Synchronisationskonten mit Replikationsrechten (Kennwort-Hash-Synchronisation)	1: ARVEN\MSOL_7f3c21e9b4d0	Konstruktionsbedingt Tier 0 (Entra Connect / Cloud Sync) — als Tier-0-Konto schützen (Server in Tier-0-OU, Kennwortabruf nur vom Sync-Server); erklärt über Privileged.ExpectedSyncAccounts (66_-Datei, Spalte Grund).
INFO	Geprüfte Angriffstechniken mit nachgewiesener Exposition	1 von 19	Details in der Angriffsflächen-Matrix (69_AttackSurface_Matrix.csv).

● Forest & Altlasten

Bewertung	Befund	Messwert	Empfehlung
INFO	Objekte mit Schlüsselaneldeinformationen (Windows Hello for Business / Hybrid Join)	1.142	Betriebsstandard bei WHfB und hybrid verbundenen Geräten; keine Maßnahme (96_-Datei).
INFO	AD-Systemstatus-Sicherung aktuell	0 Tage	Unmittelbar vor dem Umbau erneut sichern (90_AD_Sicherung.csv).
INFO	Replikation fehlerfrei	0 Fehler	Erwartetes Bild (90_Replikation.csv).

● Tiering & Administration

Bewertung	Befund	Messwert	Empfehlung
HOCH	Aktive Tier-0-Konten nicht in "Protected Users" QF	7	In Wellen aufnehmen (kein NTLM, kein RC4, keine Delegation, 4-h-TGT) — Betriebskonten vorher testen (75_-Datei, Spalte InProtectedUsers = False; PingCastle P-ProtectedUsers).
INFO	Authentication Mechanism Assurance nicht konfiguriert	keine OID-Gruppen-Verknüpfung	AMA koppelt Autorisierung an die Authentifizierungsart — Kompromittierung ohne Karte bleibt folgenlos.
INFO	Effektive Tier-Wirkung der Gruppen (gemessen, nicht nach Namen)	Tier 0: 4 · Tier 1: 21 · Tier 2: 3 · mehrere: 0 · ohne Wirkung: 1.068	Grundlage für ein Rollenmodell je Tier; Tier 2 heute: Delegationen auf Client-OUs (130_).

Bewertung	Befund	Messwert	Empfehlung
INFO	Adminkonten-Kontosicht: Namensmuster, Tier-Wirkung, Schutz, Sync, lokale Rechte und Cloud-Rollen je Konto	38 Adminkonten (Muster, Tier-0-Wirkung oder Cloud-Rolle) · Tier 0	Eine Zeile je Konto mit allen Fakten in 238_Adminkonten.csv (Muster nach Tiering.AdminAccountNamePatterns/AdminAccountTierPatterns) . Die Bewertung der Einzelpunkte (Postfach, delegierbar, Protected Users) steht in den bestehenden Befunden; die Zuordnung Name ↔ Tier wird ausgegeben, nicht bewertet. 14, davon ohne Adminmuster 0 · mit Postfach 0 · Tier 0 delegierbar 0 · ohne Ablaufdatum 9
INFO	Personenmatrix: Alltagskonto ↔ Adminkonten	31 Personen mit zugeordneten Adminkonten · 0 Adminkonten ohne zuordenbares Personenkonto · 0 Personen mit mehreren Konten gleicher Wirkung · 12 Personen mit lokalen Adminrechten auf Servern	Zuordnung über employeeID, manager, Beschreibung, Namensbestandteil und Anzeigename (Spalte Zuordnungsweg); unzugeordnete Adminkonten sind Kandidaten für Rezertifizierung oder technische Konten (239_Personen_Kontenmatrix.csv, 238_ Spalte Person).

● Server: lokale Gruppen

Bewertung	Befund	Messwert	Empfehlung
INFO	Firewall-Freischaltungen für den WinRM-Scan erforderlich (TCP 5985 vom Scan-System)	2 Subnetze	Regeln in 108_Firewall_Bedarf.csv (Spalte Regel); Nachweis je Server in 107_ (Timeout = Firewall, abgelehnt = WinRM-Dienst). 10.20.40.0/24 (AW-Werk-Sued), 10.20.60.0/24 (AW-Labor)
INFO	Abdeckung der Servererhebung	94 von 96 Servern gelesen, 2 nicht erreichbar	Nicht erreichbare Server: WinRM-Erreichbarkeit oder Berechtigung des Scan-Kontos (105_LocalGroups_NichtErreichbar.csv).
INFO	Klassifikation der lokalen Gruppenmitglieder je Server	412 Einträge klassifiziert · 88 von 94 Servern nur mit erwarteten Gruppen · 12 Personen über verschachtelte Domänengruppen in Administratoren · 0 verwaiste SIDs	Ist-Bild je Server (EINGEBAUT, ERWARTET, DOMÄNENGRUPPE, PERSON_DIREKT, VERSCHACHELTELT, FREMDE_SID ...) in 231_LokaleGruppen_Mitglieder.csv; Zusammenfassung je Server in 106_LocalGroups_JeServer.csv (Spalten Klasse*, NurErwarteteGruppen).

● Kennwort-Hygiene

Bewertung	Befund	Messwert	Empfehlung
INFO	Aktive Computerkonten mit Maschinenkennwort zwischen 45 und 90 Tagen	11	Rotation läuft verspätet (Standard 30 Tage) — Systeme mit langer Offline-Zeit oder abgeschalteter Rotation (26_-Datei, Bewertung AUFFÄLLIG; PingCastle S-PwdLastSet-45).

● Protokoll-Härtung

Bewertung	Befund	Messwert	Empfehlung
INFO	Härtung Stufe 2: Sollwerte gegen wirksame GPO-Einstellungen je OU geprüft	59 Regeln auf 1.214 Computern: 56 erfüllt, 0 teilweise, 3 Lücken; mittlere Abdeckung 91 %	Je Regel: Abdeckung nach Computern, Beispiel-GPO und abweichender Wert (181_Haertung_Uebersicht.csv); je OU (180_) — Grundlage für die Baseline-GPOs des Neuaufbaus.
WARN	Weitere Härtingsregeln ohne Wirksamkeit	3	NTLM: eingehenden Datenverkehr einschränken; NTLM: Authentifizierung in dieser Domäne einschränken (DC); LDAP-Clientsignatur erforderlich (181_-Datei)

Konten & Aktivität

Bewertung	Befund	Messwert	Empfehlung
WARN	Aktivierte Konten ohne Anmeldung (AD UND Entra, effektiv inaktiv) QF	64	Freigabeprozess starten (Modul 2), dann staged deaktivieren (Modul 3).
INFO	Konten, die nur dank Entra-Abgleich NICHT als Löschkandidat geführt werden	312	Beleg für die Notwendigkeit des hybriden Abgleichs.

Lizenzen

Bewertung	Befund	Messwert	Empfehlung
WARN	Lizenzierte, aber effektiv inaktive Konten QF	23	Lizenz-Reclaim sofort möglich (Quick Fix) - siehe Wertrechner.

Gruppen & Token

Bewertung	Befund	Messwert	Empfehlung
WARN	Leere Gruppen QF	61	Nach Prüfung löschen (Quick Fix).
INFO	Gruppen-Verwendungsmatrix erstellt (wofür wird jede Gruppe heute verwendet)	1.096 Sicherheitsgruppen	140 Gruppen_Verwendung.csv = je Gruppe alle Verwendungsstellen mit Empfehlung für den Neuaufbau (übernehmen, umbauen, klären, löschen). 84 tragen Berechtigungen (ACL, GPO, lokale Servergruppen), 471 reine Rollengruppen, 24 mit Mitgliedern ohne erkennbare Verwendung, 58 ohne Verwendung und Mitglieder
INFO	Gruppen mit Mitgliedern, deren Verwendung im Scan nicht sichtbar ist (Dateiserver, Anwendungen, Datenbanken)	24	Vor der Migration je Gruppe klären — Kandidaten für Dateisystem-ACL-Scan oder Rückfrage bei den Anwendungsverantwortlichen (140_-Datei, Verwendungsart "Verwendung nicht ermittelbar").

Privilegien & Delegation

Bewertung	Befund	Messwert	Empfehlung
INFO	Delegationsmodell: OU-Admin-Gruppen mit Vollzugriff auf ihre Teilbäume (Tier 1, laut Config gewollt)	9	Kein Eskalationsfund, aber Tier-1-Vollzugriff: Mitglieder halbjährlich rezertifizieren, keine Tier-0-Objekte in diesen Teilbäumen ablegen (64_-Datei, Herkunft "Delegationsmodell").
INFO	Hochrisiko-Rechte von Produktkonten (Entra Connect, Exchange, Lync, Windows-Standard)	2	Produktstandard; nur prüfen, ob das Produkt noch im Einsatz ist und ob die Konten selbst gehärtet sind.
INFO	Effektiv privilegierte Benutzer (transitiv)	6 (davon 6 aktiviert, 0 deaktiviert)	Regelmäßig rezertifizieren; deaktivierte Mitglieder aus den Gruppen entfernen (60_-Datei).
INFO	Effektives Tier 0: vom Kunden erklärte Prinzipale (Sync-Konten, konfigurierte Tier-0-Gruppen)	1 erklärt, 0 unerklärt	Erklärt heißt nicht entwarnt: die Rechte bleiben Tier 0 und die Prinzipale brauchen Tier-0-Schutz. Erklärt: MSOL_7f3c21e9b4d0 (Entra Connect) (61_Tier0_Effektiv.csv, Spalten Erwartet/Grund)
INFO	Delegationsinventar erstellt (wer darf was wo — Grundlage für das neue Rollenmodell)	164 definierte Delegationen an 23 Prinzipale	133_ = Aufgabenkatalog mit Rollenvorschlag, 132_ = je Prinzipal, 131_ = wirksam je OU, 130_ = wo definiert. Neue Struktur: je Aufgabe und OU-Bereich eine Rollengruppe (AGDLP), Personen nur über Rollen. 41 unterscheidbare Aufgaben, wirksam auf 58 OUs/Containern
INFO	Domain Join: wer Computerkonten anlegen darf	3 Prinzipale; 0 dürfen bestehende Konten übernehmen; MachineAccountQuota = 0	Zielbild: eine Join-Rolle je Standort-OU, MachineAccountQuota 0, Benutzerrecht 'Hinzufügen von Arbeitsstationen' nur für diese Rolle. Heute: ARVEN\AW-T1-DomainJoin-Nord, ARVEN\AW-T1-DomainJoin-Sued, ARVEN\gmsa-osd\$
INFO	Verweigern-Einträge in OU-Berechtigungen	41	Deny-ACEs verdecken Rechte und überleben Umbauten unbemerkt — beim Neuaufbau einzeln prüfen und möglichst durch fehlende Allow-Rechte ersetzen (134_-Datei).

Bewertung	Befund	Messwert	Empfehlung
INFO	Änderungen an privilegierten Gruppen in den letzten 90 Tagen	2 hinzugefügt, 5 entfernt	Ans Replikationsmetadaten rekonstruiert (auch ohne Ereignisprotokoll) — mit Tickets abgleichen (191_-Datei).

● Delegation & Rechte

Bewertung	Befund	Messwert	Empfehlung
INFO	Konten mit Kerberos-Delegation (constrained/RBCD)	4	Zieldienste regelmäßig rezertifizieren (65_Delegation_Kerberos.csv).

● Passwort-Richtlinien

Bewertung	Befund	Messwert	Empfehlung
INFO	Wirksame Kennwortrichtlinie je Konto (Domänenrichtlinie / PSO)	1.455 unter Domänenrichtlinie, 57 unter PSO (2 PSOs)	Verteilung der erzwungenen Mindestlänge (Länge: Konten): 14: 1455, 20: 57. Dienstkonten unter Domänenrichtlinie: 0, Adminkonten unter Domänenrichtlinie: 0 (15a_FGPP.csv, 15b_Kennwortrichtlinie_JeKonto.csv).

● GPO

Bewertung	Befund	Messwert	Empfehlung
WARN	Wirkungslose GPOs (leer / unverlinkt / deaktiviert / leeres Filtering) QF	12 von 84	Nach Sichtung entfernen - reine Verwaltungslast (siehe Wertrechner).
INFO	GPO-Einstellungsinventar erstellt (Grundlage für neue GPOs bei OU-Umbau)	1.406 Einstellungen in 84 GPOs, wirksame Menge für 61 OUs/Container mit Objekten	120_ = alle Einstellungen, 123_ = wirksamer Wert je OU und Einstellung mit Quell-GPO — beim Neuaufbau je Ziel-OU übernehmen; Loopback und deaktivierte Hälften sind berücksichtigt.
INFO	Sammel-GPOs mit vier und mehr Einstellungsbereichen	4	Beim Neuaufbau thematisch trennen (Baseline Sicherheit, Baseline Clients, Anwendungen) — erleichtert Störungssuche und Delegation (121_-Datei).
INFO	Identische Einstellungen in mehreren GPOs (Konsolidierungskandidaten)	97	In eine gemeinsame Baseline-GPO überführen (125_GPO_Duplikate.csv).
INFO	OUs mit Loopback-Verarbeitung (Benutzereinstellungen der Computer-Kette wirken)	2	Typisch Terminalserver/Citrix — beim Neuaufbau die Benutzereinstellungen dieser Ketten mitnehmen (122_GPO_Loopback_OUs.csv).
INFO	Keine GPO-Einstellung verweist auf OU-/Container-Pfade	0	OU-Umbau ohne GPO-Inhaltsanpassung möglich (Verknüpfungen bleiben natürlich neu zu setzen).

● Neuaufbau: Grundlagen

Bewertung	Befund	Messwert	Empfehlung
INFO	Sync-Scope je OU eindeutig (vollständig oder gar nicht synchronisiert)	21 OUs im Scope, 14 außerhalb	Für den Umbau trotzdem Attributfilter statt OU-Filter erwägen — dann ist die Sync-Zugehörigkeit unabhängig vom Standort im Verzeichnis (47_-Datei).
INFO	Freie Erweiterungsattribute für ein Sync-Flag verfügbar	11	Kandidaten: extensionAttribute9, extensionAttribute10, extensionAttribute11, extensionAttribute12, msDS-cloudExtensionAttribute1 — eines davon als Sync-Kennzeichen festlegen und im Entra-Connect-Filter verwenden (18_Attribute_Belegung.csv)
INFO	OUs mit gemischtem Inhalt (Server und Clients / Benutzer und Computer)	1 / 0 von 56 OUs mit Objekten	Objektklassen je OU als Grundlage für OU-Struktur und GPO-Zuschnitt — gemischte OUs erlauben keine klassenreinen Richtlinien (235_OU_Inhalt.csv). Server und Clients gemischt: OU=Labor,OU=Werk-Sued,OU=Arvenwerk,DC=arvenwerk,DC=local
INFO	Dienstkonten: Pflegegrad der Attribute (Verantwortlicher, Beschreibung, Ablauf, Anmeldebeschränkung, Silo, AES-only)	19 Dienstkonten	Ist-Stand je Dienstkonto in 12_Users_ServiceAccounts.csv (Spalten ManagedBy, LogonWorkstations, AuthPolicySilo, KerberosEncTypes, AesOnly, SpnHosts). 19 mit managedBy, 19 mit Beschreibung, 0 mit Ablaufdatum, 11 mit LogonWorkstations, 0 im Silo, 17 AES-only

● Entra-Security

Bewertung	Befund	Messwert	Empfehlung
WARN	Abgelaufene App-Anmeldeinformationen QF	14	14 abgelaufene Secrets/Zertifikate (Hygiene/Betriebsrisiko). Quelle: 85_Entra_SecurityFindings.csv
WARN	Inaktive Gastkonten QF	142	142 aktivierte Gastkonten ohne Anmeldung seit >90 Tagen (oder nie). Quelle: 85_Entra_SecurityFindings.csv
INFO	PIM-berechtigte Zuweisungen (eligible)	25	25 eligible Zuweisungen über PIM, davon 4 Global Administrator (81_Entra_RoleEligible_PIM.csv).
INFO	Permanente Rollenzuweisungen (gesamt)	18	18 permanente Zuweisungen neben 25 eligible - permanente Zuweisungen außer Break-Glass und Dienstkonten in PIM überführen (81_Entra_RoleMembers.csv).
INFO	GÄSTE OHNE SPONSOR	38	38 aktivierte Gastkonten ohne Sponsor - niemand ist für Zugriffsüberprüfung und Abmeldung verantwortlich (84_Entra_Guests.csv, Spalte Sponsors).

● Entra: Admin-Modell & Tenant

Bewertung	Befund	Messwert	Empfehlung
WARN	Benutzer nur mit Telefon/SMS/E-Mail als MFA	37	37 Mitgliedskonten nur mit Telefon/SMS/E-Mail als MFA. Authenticator mit Number Matching als Mindeststandard, SMS/Anruf schrittweise abschalten. Quelle: 159_Entra_AdminModel_Findings.csv (Details 150_-158_)
INFO	Benutzerdefinierte Rollen	1	1 benutzerdefinierte Rollen (0 mit weitreichenden Aktionen): Helpdesk Kennwortrücksetzung Werk (151_Entra_CustomRoles.csv)
INFO	Ungenutzte Lizenzen je SKU	4	4 SKUs mit mehr als 10 % freien Lizenzen: VISIOCLIENT 9/40, PROJECTPROFESSIONAL 6/25, POWER_BI_PRO 12/60, Microsoft_Teams_Rooms_Pro 2/8. Bei Verlängerung reduzieren (158_Entra_Lizenzen_SKU.csv).
INFO	Microsoft Secure Score	-	Microsoft Secure Score 318.40 von 373.0 (85 %). Größte offene Identity-Kontrollen: Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other eligible servers. (+5); Ensure custom banned passwords lists are used (+5) (157_Entra_SecureScore.csv)
INFO	Vertrauenswürdige Standorte (MFA-Umgehung prüfen)	2	2 als vertrauenswürdige markierte Standorte: Werk Nord NAT [203.0.113.10/32]; Werk Süd NAT [198.51.100.20/32] (152_Entra_NamedLocations.csv)
INFO	Administrative Units im Einsatz	3	3 Administrative Units, 4 auf AUs eingeschränkte Rollenzuweisungen (151_Entra_AdministrativeUnits.csv).
INFO	Lizenzen direkt statt gruppenbasiert zugewiesen	46	46 Benutzer mit direkt zugewiesenen Lizenzen (1.394 rein per Gruppe). Gruppenbasierte Lizenzierung über die neuen Rollengruppen macht Offboarding und Sync-Scope-Änderungen lizenzneutral (158_Entra_Lizenzzuweisung.csv).

● Entra: Apps & Berechtigungen

Bewertung	Befund	Messwert	Empfehlung
INFO	Anwendungen ohne Anmeldung (Bereinigung) QF	37	37 eigene/Drittanbieter-Anwendungen ohne Anmeldung seit > 180 Tagen - Bereinigungskandidaten (160_-Datei).
INFO	SSO-Anwendungen ohne Zuweisungspflicht	3	3 eigene SSO-Anwendungen ohne Zuweisungspflicht - jeder Benutzer des Tenants kann sich anmelden; Zugriff über Gruppen zuweisen (160_-Datei, ZuweisungErforderlich).
INFO	Scan-App des Identity Health Checks	-	Die Scan-App 'Identity Health Scan' hat 18 Application Permissions (höchste Stufe MITTEL) - nach Projektende Secret löschen bzw. App entfernen. Quelle: 169_Entra_Apps_Findings.csv (Details 160_-163_)
INFO	Anwendungen mit föderierten Anmeldeinformationen (Workload Identity Federation)	12	12 App-Registrierung(en) nutzen föderierte Anmeldeinformationen (Workload Identity Federation, 15 Einträge) - je Eintrag prüfen: nur erwarteter Aussteller, kein breites oder fremdes Subjekt (164_Entra_App_FederatedCredentials.csv).

● **Entra: Geräte & Sync**

Bewertung	Befund	Messwert	Empfehlung
WARN	Inaktive Geräteobjekte QF	96	96 aktivierte Geräte ohne Aktivität seit > 180 Tagen. Veraltete Geräteobjekte erfüllen CA-Gerätebedingungen weiter und verfälschen Compliance-Zahlen - deaktivieren, nach 30 Tagen löschen (170_Entra_Geraete.csv).
INFO	Registrierte (BYOD) Geräte	214	214 registrierte (Workplace-joined) Geräte - private/nicht verwaltete Geräte mit Zugriff; Zugriff per CA auf App-Schutzrichtlinien begrenzen. Quelle: 179_Entra_Devices_Findings.csv (Details 170_-174_)
INFO	Geräte ohne MDM-Verwaltung	6 von 1.188	6 von 1.188 aktiven Entra-/Hybrid-Geräten ohne MDM-Verwaltung (1 %). Ohne Verwaltung keine Compliance-Bedingung in CA möglich. Quelle: 179_Entra_Devices_Findings.csv (Details 170_-174_)
INFO	Aktive Geräte ohne bewertbare Betriebssystemversion	9	9 aktive Geräte ohne bewertbare Betriebssystemversion (Linux, fehlende Version, unbekannter Build) - Mindestversionen in Entra.DeviceMinOsVersions pflegen. Quelle: 179_Entra_Devices_Findings.csv (Details 170_-174_)
INFO	Sync-Scope Computer: Hybrid-Geräte vs. AD-Clients	1.118	1.118 aktive AD-Clients: 1.112 hybrid-gejoint (müssen im Sync-Scope bleiben), 6 ohne Entra-Gerät (aus dem Scope nehmen oder Hybrid Join nachholen). Je OU: 172_AD_SyncScope_Computer_JeOU.csv, je Computer: 172_AD_Computer_SyncScope.csv.

● **Compliance: DORA**

Bewertung	Befund	Messwert	Empfehlung
HOCH	DORA / RTS (EU) 2024/1774 - Identitäts- und Zugangsmanagement (mit BAIT-Querverweis): PFLICHT-Regeln mit Befund	3 von 21	Nachweis nicht erbracht - PFLICHT-Regeln mit Befund vor der nächsten Prüfung schließen. Offen: DORA-RTS20.1, DORA-RTS21d.3, DORA-RTS21f.2 (203_DORA_Compliance.csv)
WARN	DORA / RTS (EU) 2024/1774 - Identitäts- und Zugangsmanagement (mit BAIT-Querverweis): PFLICHT-Regeln ohne Nachweis (nicht prüfbar oder nicht abgedeckt)	0 nicht prüfbar, 2 nicht abgedeckt	Nicht prüfbar = Modul im Lauf übersprungen oder Recht fehlte; nicht abgedeckt = Toolkit prüft die Regel (noch) nicht, Begründung in Spalte Hinweis. Regeln: DORA-RTS20.3, DORA-RTS21e.5 (203_DORA_Compliance.csv)

Angriffsflächen-Matrix

Geprüft wird, ob die technischen **Voraussetzungen** bekannter Angriffstechniken in der Umgebung vorliegen — ausschließlich durch Lesen der AD-Konfiguration, ohne jeden aktiven Test. Status „EXPONIERT“ bedeutet: Die Konfiguration ermöglicht diese Technik. Einträge mit „EMPFEHLUNG“ oder „DETEKTION PRÜFEN“ sind aus der Konfiguration nicht ableitbar und betreffen Monitoring bzw. Auditing.

Technik	Status	Feststellung	Gegenmaßnahme
Reconnaissance			
dSHeuristics: Verzeichnisweite Sicherheitsschalter	TEILWEISE	dSHeuristics='0000000001000000000200000011': AdminSDExMask=False, LDAP-Sicherheit 28/29=True, SIDHistory-Standardisierung aus=False, UPN/SPN-Eindeutigkeit aus=False, ListObject=False	dwAdminSDExMask = 0, LDAPAddAuthZVerifications/LDAPOwnerModify = 1 (KB5008383), Migrationsschalter nach Abschluss zurücksetzen.
LDAP-Enumeration ohne Anmeldung	GESCHÜTZT	dSHeuristics ohne Freigabe anonymer LDAP-Operationen (Zeichen 7 = 0)	dSHeuristics zurücksetzen; anonyme Bindungen unterbinden.
Verzeichnis-Auslesen über Alt-Kompatibilitätsgruppe	GESCHÜTZT	Pre-Windows 2000 Compatible Access enthält nur Authentifizierte Benutzer	Everyone/Anonymous/Authenticated Users aus der Gruppe entfernen.
Benutzer-Enumeration über Kerberos (Port 88)	DETEKTION PRÜFEN	Aus der AD-Konfiguration nicht feststellbar - hängt an Monitoring/SIEM	Event 4768 auf DCs auswerten: viele Anfragen mit Fehler 0x6 (unbekannter Principal) von einer Quelle = Enumerationsversuch. SIEM-Regel einrichten.
Massenhafte LDAP-Abfragen (Mapping-Werkzeuge)	DETEKTION PRÜFEN	Alle DCs beantworten LDAP-Abfragen gleichermaßen	ALLE DCs ins Monitoring aufnehmen (nicht nur die primären); Event 5145 und ungewöhnliche SPN-/Massenabfragen alarmieren.
Persistenz			
Domänen-Root-ACL: bekannte Fehlmuster (Key Admins Vollzugriff, Exchange WriteDacL)	GESCHÜTZT	Keine bekannten Fehlmuster auf der Domänen-Root-ACL (Exchange nur als Exchange Online, Key Admins auf msDS-KeyCredentialLink beschränkt)	Key Admins: ACE auf msDS-KeyCredentialLink beschränken (KB4088889); Exchange: Split-Permissions-Modell oder WriteDacL-ACE entfernen.
Verzeichnis-Replikation missbrauchen (DCSync)	GESCHÜTZT	Nur erwartete Standardgruppen und das Entra-Connect-Konto besitzen Replikationsrechte (9 ACEs geprüft)	Replikationsrechte ausschließlich DCs und Tier-0 belassen; Event 4662 auf Replikations-GUIDs alarmieren.
Credential-Angriffe			
Service-Ticket-Angriff (Kerberoasting)	TEILWEISE	4 aktive Dienstkonten mit SPN, davon 0 privilegiert und 0 ohne erzwungenes AES	Dienstkonten auf gMSA umstellen (automatische Langpasswörter); privilegierte Konten nie mit SPN betreiben; AES erzwingen; Honeypot-SPN als Frühwarnung.
Schwache Kerberos-Verschlüsselung (RC4/DES) je Prinzipal	GESCHÜTZT	0 Prinzipale explizit nur RC4/DES, 0 mit DES-Bits, keine Vertrauensstellungen; DefaultDomainSupportedEncTypes = AES	AES128/256 setzen, DES-/RC4-only-Werte entfernen; Trusts mit "The other domain supports Kerberos AES encryption"; DefaultDomainSupportedEncTypes vor der RC4-Abschaltung prüfen.
Lateral Movement			
Wiederverwendung gestohlener Tickets (Pass-the-Ticket)	ÜBLICH	MaxTicketAge=10h, MaxRenewAge=7d	Ticketlaufzeiten auf Standard (10 h / 7 d) begrenzen; Tier-0-Konten in Protected Users (Tickets nicht delegierbar).
Credential-Angriffe			
Passwort-Spraying (ein Passwort gegen viele Konten)	GESCHÜTZT	LockoutThreshold=5, MinPasswordLength=14, Beobachtungsfenster=15 min	Mindestlänge >= 12 Zeichen, Sperrschwelle aktiv, verbotene Passwortmuster (Banned-Password-Liste); Alarm auf viele Fehlanmeldungen verschiedener Konten aus einer Quelle (Event 4625).
Angriff ohne Anmeldung (AS-REP Roasting)	GESCHÜTZT	0 aktive Konten ohne Kerberos-Vorauthentifizierung, davon 0 privilegiert	Vorauthentifizierung für alle Konten aktivieren - insbesondere privilegierte.
Persistenz			
Fälschung von Kerberos-Tickets (Golden Ticket)	GESCHÜTZT	krbtgt-Passwort seit 63 Tagen unverändert (Schwelle 180 Tage)	krbtgt zweimal rotieren (Abstand > 10 h); danach sind alte gefälschte Tickets wertlos.
Rechteauserweiterung			

Technik	Status	Feststellung	Gegenmaßnahme
Missbrauch unbeschränkter Delegation	GESCHÜTZT	0 aktivierte Objekte (ohne DCs) mit unbeschränkter Delegation	Auf beschränkte Delegation umstellen oder entfernen; Tier-0 in Protected Users ("Konto ist vertraulich").
Lateral Movement			
Weiterverwendung von Passwort-Hashes (Pass-the-Hash)	EXPONIERT	LAPS: vorhanden (Windows LAPS, 1.203 von 1.210 Computern) Mitglieder in Protected Users: 7 NTLM auf DCs nicht eingeschränkt	LAPS flächendeckend einführen; Tier-0 in Protected Users; NTLM einschränken; Admin-Anmeldungen auf Arbeitsplätzen unterbinden.
Rechteauserweiterung			
Übermäßige Gruppen- und Delegationsrechte	SIEHE DETAILANALYSE	Auswertung in Modul 10 (effektive privilegierte Mitglieder, OU-Delegationen)	Least Privilege durchsetzen, Tier-Modell, regelmäßige Rezertifizierung.
Detektion			
Früherkennung Kerberoasting	EMPFEHLUNG	Nicht aus der Konfiguration ableitbar	Honeypot-SPN anlegen (Dienstkonto ohne echten Dienst): jede Ticketanfrage darauf ist verdächtig; Event 4769 mit RC4-Verschlüsselung alarmieren.
Früherkennung DCSync	EMPFEHLUNG	Nicht aus der Konfiguration ableitbar	Event 4662 auf Replikations-GUIDs alarmieren, wenn der Aufrufer kein DC ist.
Früherkennung Enumeration und Spraying	EMPFEHLUNG	Nicht aus der Konfiguration ableitbar	Event 4768 (Fehler 0x6) und 4625 korrelieren; alle DCs einbeziehen, nicht nur die primären.

4b · Diagramme

Ist-Darstellung aus den Kennzahlen dieses Laufs. Ein Pfad ist eine Möglichkeit laut Rechten und Mitgliedschaften, kein Nachweis einer Ausnutzung. Quelltext je Diagramm in 245_Diagramme/*.mmd.

Angriffspfade zu Tier 0 (Ist-Möglichkeiten laut Rechten)

```
flowchart LR
    DU["Domaenen-Benutzer"]:::broad
    AU["Authentifizierte Benutzer"]:::broad
    USR["Aktive Benutzer mit Pfad<br/>0"]:::src
    T0["Tier 0<br/>22 Ziele"]:::tier0
    UD["Unbeschraenkte Delegation<br/>0"]:::tier0
    AU --> USR
    classDef broad fill:#ffcdd2,stroke:#b71c1c;
    classDef src fill:#fff3e0,stroke:#e65100;
    classDef choke fill:#fff9c4,stroke:#f9a825;
    classDef tier0 fill:#c8e6c9,stroke:#2e7d32;
```

Relay-/Coerce-Exposition

```
pie showData title Relay-/Coerce-Kanaele (Ist)
    "Exponiert" : 3
    "Teilweise" : 1
    "Gemindert" : 7
    "Nicht pruefbar" : 1
```

Tier-0-Konten: Schutzlage

```
flowchart TB
    ALL["Tier-0-Konten gesamt<br/>14"]:::t0
    DEL["delegierbar<br/>0"]:::warn
    NP["nicht in Protected Users<br/>7"]:::warn
    ALL --> DEL
    ALL --> NP
    classDef t0 fill:#c8e6c9,stroke:#2e7d32;
    classDef warn fill:#ffe0b2,stroke:#e65100;
```

4c · Mehrlauf-Trend

Entwicklung ausgewählter Kennzahlen über alle 6 Läufe dieses Kunden. Ist-Werte ohne Bewertung; Sollwerte gehören dem Kundenprojekt.

Kennzahl	20260504_0600	20260601_0600	20260706_0600	20260803_0600	20260907_0600	20261005_0600
Effektiv inaktive Konten	212	148	97	81	70	64
Hochrisiko-Delegationen	31	22	14	10	9	9
Wirkungslose GPOs	41	33	24	18	15	12
Tier-0 delegierbar	11	6	2	0	0	0
SIDHistory-Objekte	186	186	40	0	0	0
Benutzer mit Pfad zu Tier 0	23	9	4	1	0	0
Exponierte Relay-Kanäle	6	5	4	3	3	3
Härtungsabdeckung Ø (%)	54	63	72	81	88	91

4 · Compliance-Nachweis

DORA / RTS (EU) 2024/1774 - Identitäts- und Zugangsmanagement (mit BAIT-Querverweis)

v4.0.0 - Mapping cosoweb · Quelle: Verordnung (EU) 2022/2554 (DORA), Art. 9 Abs. 4 lit. c und d; Delegierte Verordnung (EU) 2024/1774 (RTS IKT-Risikomanagementrahmen), Titel II Art. 12 (Datenaufzeichnung), Art. 20 (Identitätsmanagement), Art. 21 (Zugangskontrolle). Querverweis BAIT Kapitel 6 (Tz. 6.1-6.8, Fassung 16.12.2024). Anwendbarkeit im Einzelfall prüfen; keine Rechtsberatung.

PFLICHT offen: 5 von 21 - 3 mit Befund, 0 nicht prüfbar, 2 nicht abgedeckt; 16 erfüllt. Alle Regeln: 3 Befund, 20 OK, 0 nicht prüfbar, 3 nicht abgedeckt. Drift gegen Arvenwerk_20260907_0600: 0 neu, 1 behoben.

Status: OK = geprüft, kein Befund · BEFUND = geprüft, Befund vorhanden · NICHT_PRUEFBAR = Prüfung vorhanden, im Lauf ohne Daten (Modul übersprungen, Recht fehlte) · NICHT_ABGEDECKT = Toolkit prüft die Regel nicht (Begründung in Hinweis). Ohne Daten nie OK. Export: 203_DORA_Compliance.csv

Regel	Titel	PFLICHT	Status	Messwert	Hinweis / Quelldatei / Drift
DORA / RTS (EU) 2024/1774					
DORA-RTS20.1	Identitätsmanagement: Lebenszyklus - inaktive Identitäten deaktiviert	PFLICHT	BEFUND	64	StaleCandidates_Effective > 0 · Quelle: 41_Users_StaleCandidates_Effective.csv · Drift: verbessert (70 → 64)
DORA-RTS20.2	Identitätsmanagement: keine aktivierten, nie genutzten Konten	PFLICHT	OK	0	UsersEnabled_NeverLoggedIn > 0 · Quelle: 10_Users_Inventory.csv
DORA-RTS20.3	Identitätsmanagement: Aufzeichnungen über alle Identitäten (auch nach Vertragsende)	PFLICHT	NICHT_ABGEDECKT	–	Aufbewahrungspflicht des Unternehmens; das Toolkit liefert je Lauf ein vollständiges Konteninventar (10_/30_) als Nachweisgrundlage, ersetzt aber kein IAM-Register.
DORA-RTS21a.1	Need-to-know/Least Privilege: keine Delegationen an breite Gruppen	PFLICHT	OK	0	DelegationsBroadTrustees > 0 · Quelle: 132_Delegationen_JeTrustee.csv
DORA-RTS21a.2	Least Privilege: keine gefährlichen erweiterten Rechte außerhalb Tier 0	PFLICHT	OK	0	DangerousExtendedRights > 0 · Quelle: 130_Delegationen_Definiert.csv
DORA-RTS21a.3	Least Privilege: kein unerklärtes effektives Tier 0	PFLICHT	OK	0	Tier0EffectiveUnexplained > 0 · Quelle: 61_Tier0_Effektiv.json
DORA-RTS21b.1	Funktionstrennung: keine toxischen Kombinationen (Wirkung in mehreren Tiers)	PFLICHT	OK	0	TierWirkungKontenTierBruch > 0 · Quelle: 232_TierWirkung.csv
DORA-RTS21b.2	Funktionstrennung: eine Person nicht mit mehreren Konten gleicher Wirkung	–	OK	0	PersonenMehrereKontenGleicheWirkung > 0 · Quelle: 239_Personen_Kontenmatrix.csv
DORA-RTS21c.1	Zurechenbarkeit: Adminkonten einer Person zugeordnet	PFLICHT	OK	0	AdminKontenUnzugeordnet > 0 · Quelle: 238_Adminkonten.csv
DORA-RTS21c.2	Zurechenbarkeit: generisches Administratorkonto (RID 500) nicht im Alltag genutzt	PFLICHT	OK	nicht genutzt	Rid500Assessment matches aktiv genutzt · Quelle: 194_Standardkonten.csv
DORA-RTS21d.1	Kontrollen gegen unbefugten Zugang: keine Pfade von Benutzern zu Domain Admins	PFLICHT	OK	0	UsersWithPathToDomainAdmins > 0 · Quelle: 212_Angriffspfade_Pfade.csv
DORA-RTS21d.2	Kontrollen gegen unbefugten Zugang: keine unerklärten Replikationsrechte (DCSync)	PFLICHT	OK	0	DcSyncUnexpectedTrustees > 0 · Quelle: 66_DCSync_Rights_DomainRoot.csv
DORA-RTS21d.3	Kontrollen gegen unbefugten Zugang: Zertifikatsvorlagen ohne Eskalationspfad (ESC1)	PFLICHT	BEFUND	1	TemplatesEsc1Published > 0 · Quelle: 87_ADCS_Templates_HighRisk.csv
DORA-RTS21e.1	Kontoverwaltung: Verantwortliche für Gruppen festgelegt	–	OK	0	GroupsWithoutManagedBy > 0 · Quelle: 56_Groups_OhneManagedBy.csv · Abdeckung teilweise

Regel	Titel	PFLICHT	Status	Messwert	Hinweis / Quelldatei / Drift
DORA-RTS21e.2	Privilegierter Zugang nur bei Bedarf: keine aktivierten, ungenutzten privilegierten Konten	PFLICHT	OK	0	Tier0InactiveEnabled > 0 · Quelle: 75_Tier0_AccountProtection.csv
DORA-RTS21e.3	Privilegierter Zugang ad hoc: Entra-Rollen ohne dauerhafte Zuweisung	–	OK	0	PimRolesPermanentAllowed > 0 · Quelle: 150_Entra_Rollen_Uebersicht.csv
DORA-RTS21e.4	Umgehender Entzug: deaktivierte Konten nicht mehr in privilegierten Gruppen	PFLICHT	OK	0	Tier0Disabled > 0 · Quelle: 75_Tier0_AccountProtection.csv · Drift: behoben
DORA-RTS21e.5	Rezertifizierung mindestens jährlich (kritische/wichtige Funktionen halbjährlich)	PFLICHT	NICHT_ABGEDECKT	–	Prozessanforderung. Das Toolkit liefert die Rezertifizierungsgrundlage (Inventar, Drift gegen den Vorlauf, 230_Kennzahlen.csv); Turnus und Abnahme dokumentiert das Unternehmen.
DORA-RTS21e.6	Getrennte Konten für administrative Aufgaben	PFLICHT	OK	0	Tier0OhneAdminNamensschema > 0 · Quelle: 75_Tier0_AccountProtection.csv
DORA-RTS21e.7	Privileged Access Management möglichst automatisiert	–	NICHT_ABGEDECKT	–	Technische Lösung (PAM/PIM on-prem) ist aus dem AD nur indirekt sichtbar; Entra-PIM-Regeln in 150_.
DORA-RTS21f.1	Starke Authentifizierung für bevorrechtigten Zugang (Entra-Admins mit MFA)	PFLICHT	OK	0	AdminsWithoutMfa > 0 · Quelle: 153_Entra_MFA_Admin.csv
DORA-RTS21f.2	Starke Authentifizierung für privilegierte AD-Konten (Smartcard/Protected Users)	PFLICHT	BEFUND	0 / 7	Tier0NotInProtectedUsers > 0 · Quelle: 75_Tier0_AccountProtection.csv · Abdeckung teilweise
DORA-Art9.4d.1	Starke Authentisierungsmechanismen: Kerberos ohne RC4/DES, kein LM/NTLMv1	PFLICHT	OK	0 / 0 / 100	Quelle: 181_Haertung_Uebersicht.csv
DORA-Art9.4d.2	Schutz kryptografischer Schlüssel: krbtgt rotiert, keine schwachen CA-Zertifikate	PFLICHT	OK	63 / 0	Quelle: 195_CA_Zertifikate.csv
DORA-RTS12.1	Protokollierung der Zugangskontrolle und des Identitätsmanagements auf DCs	PFLICHT	OK	100 / 100 / 100 / 100 / 100	Quelle: 181_Haertung_Uebersicht.csv
DORA-RTS12.2	Änderungen privilegierter Gruppen nachvollziehbar (Inventar)	–	OK	2	PrivGroupChangesRecentAdded inventar 0 · Quelle: 191_PrivGruppen_Aenderungen.csv

5 · Roadmap (Reifegradmodell)

Aktuelle Einstufung: **Stufe 2 - bereinigt in Teilen, Härtung offen**

Stufe	Zustand	Weg dorthin (Produktmodul)
0 → 1	Getrennte Admin-Konten, Break-Glass	Tier-Modell Starter
1 → 2	Bereinigt (Konten, Gruppen, GPOs, Lizenzen)	Cleanup-Paket + Quick-Fix-Sprint
2 → 3	Gehärtet (Tier-0-Isolation, CA-Baseline, PIM, Legacy-Auth aus)	AD-Hardening + Entra-Security-Baseline
3 → 4	Laufende Governance (Drift-Kontrolle, Reviews, JML)	Governance-Abo

6 · Anhang

Alle Detaildaten liegen als CSV im Scan-Ordner: 10–21 Konten · 30–32 Entra · 40–47 Hybrid-Abgleich · 50–55 Gruppen/Token · 60–64 Privilegien/Delegation · 70–76 GPO · 80–86 Entra-Security · 90–98 Forest/Posture · 100–108 Server · 120–127 GPO-Einstellungen · 130–135 Delegationsinventar · 140–141 Gruppen-Verwendung · 150–179 Entra Admin-Modell/Apps/Geräte. Methodik: Scans read-only; Token-Größe geschätzt nach MS KB 327825; Aktivität = Maximum aus AD lastLogonTimestamp und Entra signInActivity. Toolkit-Version 4.0.1.