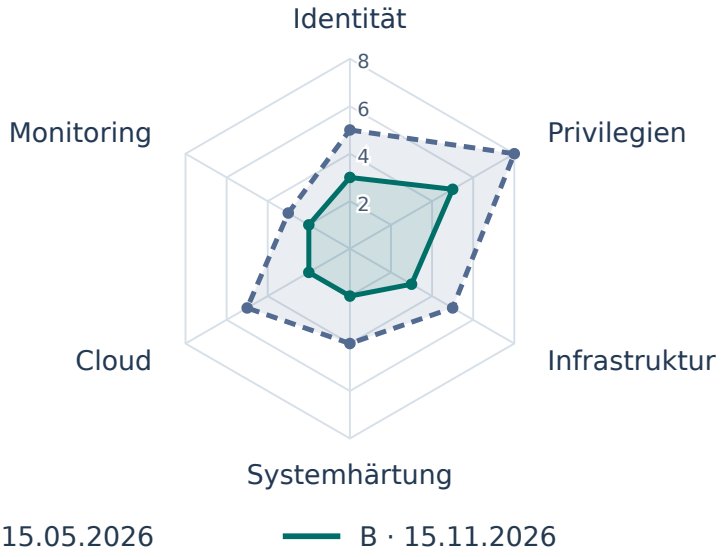
Musterwerk GmbH

Managementbericht

Scan-Vergleich / 15.05.2026 → 15.11.2026 / Purple Knight · Active Directory · demo

Im ausgewählten Prüfbereich wurden in Stand A 30 und in Stand B 17 Befunde erfasst. 0 sind in B neu hinzugekommen, 13 werden dort nicht mehr gemeldet.

Offene Befunde nach Sicherheitsbereich



Bereich	A	B	Δ
Identität & Authentifizierung	5	3	-2
Privilegierter Zugriff & Delegation	8	5	-3
AD-Infrastruktur & PKI	5	3	-2
Systemhärtung (Server & Clients)	4	2	-2
Cloud · Entra ID & Microsoft 365	5	2	-3
Überwachung & Wiederherstellung	3	2	-1

Gezählt werden gemeldete Befunde pro Bereich. Null bedeutet, dass der Scan dort keinen Befund meldet. Die Prüfabdeckung kann je Quelle variieren. In B sind 0 Befunde keinem Bereich zugeordnet und 0 ohne Schweregrad.

Prioritäten für Stand B

P1 · Privilegierte AD-Konten

DCSync-Rechte (Replicating Directory Changes All) auf Standardprinzipale beschränken – unbekannte Inhaber sofort untersuchen (5 Befunde)

P1 · Zertifikatsdienste (AD CS)

Vorlagen mit ‚Supply in request' (ESC1) deaktivieren oder Genehmigungspflicht aktivieren (3 Befunde)

P1 · Privilegierte Cloud-Konten

Privilegierte Entra-Rollen auf das Nötige reduzieren (Ziel: < 10 Rolleninhaber, Global Admin 2–4) (2 Befunde)

Datengrundlage

Stand	Scan-Datum	Quelldatei	Befunde
A	15.05.2026	Musterwerk-Demoscan-2026-05-15.csv	30
B	15.11.2026	Musterwerk-Demoscan-2026-11-15.csv	17

Verglichen werden Befundkennungen innerhalb derselben Scanreihe. „Entfallen" bedeutet, dass der Befund im gewählten Stand B fehlt. Die Behebung lässt sich mit einem gezielten Nachtest bestätigen. Bei mehrfach belegten Kennungen bleibt die Zuordnung offen.

Erstellt von Matthias Totzauer · IT Consulting Totzauer