

AUDIT-11 — Scope

Stand: 2026-05-18

Bedrohungs-Modell

Wir simulieren drei Angreifer-Profile:

Profil	Beschreibung	Zugang
A1 — Authentifizierter Koordinator	gültiger Koordinator-Account mit aktiver Session	Koordinator-Cookie + bekannte URL-Pfade
A2 — Authentifizierter Hersteller	gültiger Hersteller-Account (read-only)	Hersteller-Cookie
A3 — Operator-Account	Plattform-Operator (administrative Rolle)	Operator-Cookie

Außerhalb dieses Audits: unauthentifizierte Angriffe (siehe AUDIT-02 OWASP) und Angriffe auf den Auth-Layer selbst (siehe AUDIT-07 Pentest).

In-Scope Test-Vektoren

Vektor	Was wir prüfen
V1 — Vorgangs-Endpoint URL-Manipulation	A1 ruft <code>/api/vorgang/{case_id_von_B}</code> mit <code>case_id</code> eines anderen Koordinators auf
V2 — Mandanten-Endpoint URL-Manipulation	A1 ruft <code>/api/mandant/{mandant_id_von_B}</code> auf
V3 — Workspace-Datei-Path-Traversal	A1 versucht relative Pfade in <code>case_id</code> -Parameter
V4 — Akte-Render-Endpoint	A1 ruft Akte-HTML/PDF eines fremden Vorgangs ab
V5 — OPL-Antwort-POST	A1 sendet Antwort auf fremdes OPL
V6 — Mail-Inbox-Bucket	A1 versucht Lesen einer Mail-Eingangs-Datei von B
V7 — LLM-Prompt-Kontext-Leak	Prompt enthält versehentlich Mandanten-Daten von B
V8 — Backup-Restore-Hörspiel	A1 stellt aus Backup einen Workspace von B wieder her
V9 — Anonymisierte Logs	A1 sieht in Pipeline-Logs PII von B

Vektor	Was wir prüfen
V10 — Session-Token	Token enthält Koordinator-Identität nicht als signiertes Claim

Out-of-Scope

Bereich	Wo geprüft
Network-Layer (TLS, Firewall, DDoS)	AUDIT-07 Pentest
Anwendungs-Sicherheit allgemein (XSS, SQLi)	AUDIT-02 OWASP ASVS L2
Daten-at-rest-Verschlüsselung	AUDIT-09 §8.5.4 (offen als AUD-5)
Sub-Verarbeiter-Daten-Trennung intern bei Mistral/Anthropic	AUDIT-06

Bezugsnormen

- ISO/IEC 27001:2022 Annex A.9.4 (Zugriffs-Kontrolle Anwendung)
- ISO/IEC 27001:2022 Annex A.13.1 (Netzwerk-Sicherheit)
- OWASP ASVS 4.0.3 V8 (Authorization)
- CSA Cloud Controls Matrix v4 — MUTPL (Multi-Tenant Isolation)
- BSI C5:2020 — BEI-04 (Daten-Isolation)