SECURITY CLEARANCE & PENETRATION TEST REPORT

KUKANILEA Enterprise OS — Version 1.6.5 (Hardened)

Datum: 26. Februar 2026
Status: SECURITY CLEARED (Enterprise Ready)
Prüfungs-Scope: Core-Architektur, SQL-Integrität, Mandantentrennung & Supply-Chain.

---

1. EXECUTIVE SUMMARY

Das System KUKANILEA wurde einem umfassenden automatisierten und manuellen Sicherheits-Audit (Red-Team Simulation) unterzogen. Alle kritischen Angriffsvektoren im Bereich der Datenintegrität und Mandantensicherheit wurden erfolgreich abgesichert. Das System erfüllt die Anforderungen für den autarken Betrieb in sensiblen Handwerks-Umgebungen.

---

2. PRÜFUNGSERGEBNISSE

Kategorie	Status	Methode	Ergebnis
SQL-Injection (SQLi)	SAFE	Adversarial Input Simulation	Alle Abfragen sind strikt parametrisiert. Bösartige OCR-Inhalte werden als reiner Text behandelt.
Tenant-Isolation (RLS)	SAFE	Session-Hijacking Simulation	Zugriff auf mandantenfremde Daten ist auf Applikationsebene physisch blockiert.
Supply-Chain Security	SAFE	pip-audit (CVE Database)	0 bekannte Schwachstellen in Drittanbieter-Bibliotheken gefunden.
Static Code Analysis	SAFE	Bandit Security Scan	Keine unsicheren Funktionsaufrufe (z.B. shell=True) im Quellcode vorhanden.
Rate Limiting	VERIFIED	Load-Testing (429 Status)	Middleware schützt die App-Logik. Aggressives Blocken auf IP-Ebene wird an die Nginx-Infrastruktur delegiert.

---

3. IMPLEMENTIERTE SCHUTZMECHANISMEN

- **Zero-Trust Identity:** RSA-4096 Signatur-Verfahren für die Lizenzprüfung.
- **Privacy by Design:** DSGVO-konformes Logging durch Hashing sensibler Identifikatoren.
- **Self-Healing Storage:** Automatischer Maintenance-Daemon zur Vermeidung von Datenbank-Fragmentierung.
- **Input-Armor:** Defensive Sanitisierung von KI-Prompts zur Abwehr von Prompt-Injection-Angriffen.

---

4. EMPFEHLUNGEN FÜR DEN ROLLOUT

Das System wird für den produktiven Einsatz auf dem ZimaBlade-Hub freigegeben. Es wird empfohlen, den mitgelieferten Nginx-Reverse-Proxy für die TLS-Terminierung und das infrastrukturelle Rate-Limiting zu nutzen.

Signiert:
KUKANILEA SecOps Team (Automated Audit)