DigiEmu Core Threat Model v1.0

Status: Normative Supporting Framework – Enterprise Edition
Scope: Structured Threat Identification & Risk Mitigation
Date: 2026-02-17

1. Purpose

This document defines the structured threat model for DigiEmu Core implementations. It identifies primary risk categories and establishes mitigation strategies required for enterprise-grade deterministic knowledge infrastructure.

2. Threat Modeling Methodology

The DigiEmu Core threat model follows STRIDE classification principles:
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege.

3. Spoofing Threats

Unauthorized identity impersonation affecting API access or tenant context. Mitigation: Strong authentication, tenant-bound identifiers, and access control enforcement.

4. Tampering Threats

Unauthorized modification of ContentVersion, Claim, or Snapshot entities. Mitigation: Immutable storage constraints and deterministic hash validation.

5. Repudiation Threats

Denial of performed actions or state transitions. Mitigation: Verifiable audit logging and signed snapshot records.

6. Information Disclosure Threats

Exposure of tenant-specific knowledge across boundaries. Mitigation: Strict multi-tenant isolation and controlled access policies.

7. Denial of Service Threats

Resource exhaustion impacting snapshot reconstruction or verification. Mitigation: Rate limiting, monitoring, and infrastructure redundancy.

8. Elevation of Privilege Threats

Unauthorized privilege escalation affecting core services. Mitigation: Role-based access control and administrative audit trails.

9. Residual Risk Considerations

Infrastructure-level compromise and operational misconfiguration remain external risks. Organizations MUST implement enterprise-grade operational safeguards.

10. Governance & Certification Alignment

Threat mitigation controls SHALL align with the DigiEmu Security Model, Audit Framework, and Certification Requirements. Major changes to threat posture require governance review.