Threat Model

System: Career Automation Insights Engine

Version: 1.0

Last Updated: October 2025

Assets

- User profiles (profiles table): subscription tier, preferences
- Saved analyses (saved_analyses table): APO results, tags
- Telemetry (apo_logs, web_vitals): latency, tokens, user_id
- API keys: GEMINI_API_KEY, ONET_USERNAME/PASSWORD, Supabase keys

Threats

1. Unauthorized access to user data (RLS bypass)
2. API key exposure in client code or logs
3. Injection attacks (SQL, prompt injection)
4. Rate limit bypass or DoS
5. Cross-site scripting (XSS) via user-generated tags

Mitigations

- RLS enforced on all user-facing tables
- API keys stored in Supabase project settings; never in repo
- Parameterized queries; input sanitization on tags and user input
- Rate limiting in Edge Functions (30 req/min default)
- CSP headers; DOMPurify for user-generated content

Residual Risks

- Prompt injection: monitor validation_warnings for anomalies
- Third-party API dependencies: O*NET, Gemini, SerpAPI

Contact

Report security issues via GitHub or /responsible-ai page.