AVENLIS

Your AI Security and Red Teaming Assistant

Outcomes We Deliver

Avenlis empowers organizations to discover and mitigate risks in LLMs and AI applications, ensuring secure deployments.

Why It Matters

AI and LLM adoption brings both opportunity and risk, here’s what matters most:

- **Attack surface** → adversarial inputs, data poisoning, model manipulation
- **Business risk** → data breaches, downtime, reputational damage
- **Audit pressure** → compliance, governance, responsible AI

What is Avenlis?

Avenlis is an AI Security & AI Red Teaming platform that helps teams:

- Discover vulnerabilities in LLMs and AI workflows
- Test resilience against prompt injection and adversarial inputs
- Mitigate risks before production deployment

Avenlis is built with 2 core modules:

- **Avenlis Copilot** → AI Security and Red Teaming assistant
- **Prompt Attack** → Simulates adversarial inputs to test AI defenses

Avenlis Copilot

AI Security Guidance: Expert recommendations for addressing AI vulnerabilities.

Adversarial Testing Insights: Strategies for attack, defense mechanisms, and risk mitigation.

Industry Framework Compliance: Integration with leading security frameworks such as MITRE ATLAS, OWASP Top 10 for LLMs 2025, and NIST AI RMF.

Avenlis Prompt Attack

Manual Testing & Tracking: Test prompts directly, track outcomes, and compare exploit techniques.

Continuously Updated Library: Access to the latest adversarial prompt techniques and jailbreaks.

OWASP-Aligned Coverage: Targets critical LLM risks such as Prompt Injection, Sensitive Information Disclosure, System Prompt Leakage, and Misinformation.

How Can Avenlis Help?

- Proactive Risk Discovery
- Comprehensive Evaluation
- Enhanced Security Posture
- Continuous Adaptation

Target Audience

- AI Security / Red Teaming Enthusiasts
- Enterprises Deploying LLMs
- AI Security / Red Teaming Experts

staterasolv.com

Try Avenlis now!

avenlis.staterasolv.com