Outpost24

AI and LLM Penetration Testing

CREST-certified AI and LLM penetration testing

Outpost24 delivers in-depth, manual penetration testing to help organizations securely adopt AI and LLM based systems. As AI-driven applications are rapidly deployed, security and development teams face new and evolving risks that cybercriminals are looking to exploit.

Outpost24's AI and LLM penetration testing enables organizations to identify vulnerabilities unique to AI and LLMs systems, including prompt layer, RAG pipelines and agent workflows. By uncovering real-world, AI-specific weaknesses, organizations can confidently deploy and scale AI while reducing emerging risks and supporting AI compliance.

Penetration Tests for AI and LLMs

- Demonstrate AI security due diligence and compliance
- Full AI attack surface security coverage
- Validate LLM features before and after production
- Audit-ready reporting mapped to the OWASP Top 10 for LLMs and AI governance frameworks
- Secure AI-powered applications before release

CREST-Certified Penetration Testing

Expert-led security testing to identify AI and LLM specific vulnerabilities such as prompt injection, agents and authentication controls.

Unified Platform, Real-Time Findings, Collaboration & Retesting

Manage AI and LLM pen tests, view findings, communicate directly with testers, generate reports, and request retesting to verify fixes in a single platform.

Actionable Results & On-Demand Reporting

Complete visibility into findings, with flexible reporting to support remediation and compliance requirements.

Compliance & Quality:

Generate audit-ready reports to demonstrate AI governance such as EU AI Act, NIST AI RMF, and emerging AI industry standards.

FIND OUT MORE