

SERVICE DESCRIPTION

AI / ML Penetration Testing

CSA Cyber's AI/ML Penetration Testing service delivers deep-dive, expert security assessments for systems that integrate or depend on artificial intelligence. From a simple web-embedded chatbot to a fully custom agentic framework with multiple autonomous agents, our specialist consultants use manual, research-led techniques to uncover vulnerabilities that automated tools routinely miss. CSA's AI / ML testing methodology is aligned to OWASP LLM Top 10 and covers the following areas:

Conversational AI & Chatbots

Security testing for chatbots embedded in web apps and APIs, focused on prompt injection, data leakage, and logic manipulation.

Agentic & Multi-Agent LLM Systems

Assessment of agent orchestration, tool-calling, inter-agent trust, and autonomous behaviours in custom agentic frameworks.

Model Hosting & Infrastructure

Cloud-hosted and self-hosted model deployments, vector stores, pipelines, and inference endpoints for configuration and integration risks.

Model & Data Security

Model extraction, poisoning, insecure fine-tuning, and training-data exposure across the full AI lifecycle.

BENEFITS

- AI/ML Security Expertise - Specialist consultants with deep experience in machine learning, offensive security, and real-world adversarial techniques.
- Research-Led Testing – Manual testing that uncovers vulnerabilities missed by automated scanners and generic pen tests.
- Complete AI Ecosystem Coverage - Assessment across models, data pipelines, agentic frameworks, hosting environments, and integration points.
- Clear, Actionable Reporting - Concise findings with realistic risk ratings and practical remediation guidance tailored to engineering teams.
- Flexible Engagement Models - From rapid chatbot reviews to full penetration testing of complex multi-agent systems, aligned to your risk profile and deployment model.



Security Operations Centre



Incident Response



Penetration Testing



Intelligence-led Pen Test



Vulnerability Assessment



Assured Service Provider
In association with
National Cyber Security Centre



CYBER ESSENTIALS PLUS



Assured Service Provider
In association with
National Cyber Security Centre



CYBER ESSENTIALS PLUS

CHECK Penetration Testing

Cyber Incident Response: Standard Level



hello@csacyber.com



csacyber.com



0300 303 4691