Cobalt

DATA SHEET

AI & LLM Application Pentest

Secure your AI & LLM apps with Cobalt's expert pentesting, targeting vulnerabilities based on the OWASP Top 10 for LLM.

The explosive adoption of AI & LLMs resulted in many organizations integrating AI into their products, presenting a significant challenge for security leaders. Traditional security approaches and tools are largely ineffective against the unique vulnerabilities of AI & LLM applications.

Security testing of AI and LLM-based applications is a critical component of responsible AI deployment. Cobalt's AI & LLM application pentesting provides a structured, in-depth assessment of vulnerabilities and leverages the OWASP Top 10 for LLM applications to ensure thorough testing. By applying deep technical expertise and proven methodologies, Cobalt ensures the integrity, reliability, and security of your AI-driven applications.

WORKS WELL WITH

- API Pentesting
- Web Application Pentesting
- Secure Code Review
- Dynamic Application Security Testing (DAST)

Benefits of AI & LLM Application Pentesting

Targeted Testing for AI & LLM-Specific Vulnerabilities	Protect your application from the most exploited AI & LLM vulnerabilities, including prompt injection, model denial of service, and prompt leaking.
Targeted API and Web Application Testing	Ensure the whole LLM application operates within expected security and performance standards by testing for any overreliance, sensitive information exposure, and other vulnerabilities.
OWASP-Driven Methodology	Apply proven methodologies from OWASP Top 10 for LLMs to ensure comprehensive testing, identifying and addressing critical vulnerabilities in AI & LLM applications.
Leading Security Experts	Members of the Cobalt Core contribute to the OWASP Top 10 for LLM Applications, giving you direct access to the experts who helped shape the methodology.

> "AI security isn't a one and done process. Continuous testing is essential to stay ahead of evolving risks, and Cobalt's expertise makes them the ideal partner for this ongoing effort."
>
> ANONYMOUS
> EDTECH

The Power of Cobalt

Cobalt provides Offensive Security Solutions for programmatic risk reduction by combining technology with human expertise to deliver unmatched speed and scale to reduce risk.

SPEED

Launch with confidence. Cobalt delivers fast, on-demand testing so you can get your ideas to market quickly without sacrificing security

- **24 Hours** to Start a Pentest
- **18 Days** on Average to Get Your Report
- **7 Day** SLA for Retesting

SCALE

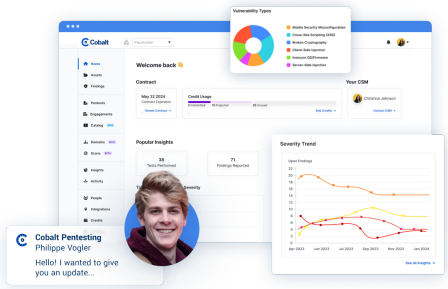
Get the efficiency of automation with the precision of experts. Broad, continuous testing across all assets; enabled by technology, optimized for growth

- **200+** Pentests Live Everyday
- **50%** of Customers do Continuous Testing
- **10k+** Critical or High Severity Vulnerabilities Discovered by Cobalt

EXPERTISE

Protect your business against evolving threats with expert-led assessments that fortify your business

- **450+ Pentesters** in the Cobalt Core
- **11 Years** of Pentesting Experience on Average
- **5% Acceptance Rate** Into the Cobalt Core

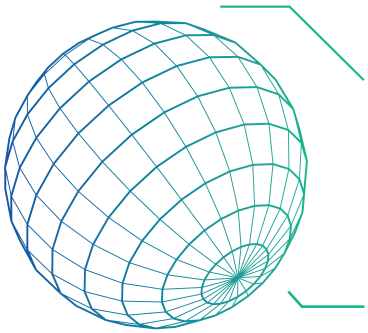


Platform

The Cobalt Offensive Security Platform centralizes access to security services from our team of expert pentesters, making it easier to find and fix vulnerabilities across your environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, on demand reporting, and seamless integration with remediation workflows, The Cobalt Platform makes it simple to build your security testing program and accelerate risk reduction.

Cobalt Core

The Cobalt Core is our community of 450+ rigorously vetted pentesters. These seasoned ethical hackers average 11 years of pentesting experience, and hold certifications such as CEH, CISSP, OSCP, and CREST. Acting as an extension of your security team, the Cobalt Core uses manual and automated offensive security tactics to uncover critical vulnerabilities through pentesting, red teaming, code reviews, and more. Reduce risk, unblock sales and new releases, and enhance your overall security posture with expert services from Cobalt.



4000+
PENTESTS DELIVERED ANNUALLY

450+
PENTESTERS

Ready to see how Cobalt leads in AI & LLM Application Pentesting?
Get started with a demo today at www.cobalt.io/get-started