InfoSight®
www.infosightinc.com

Know Exactly What Your AI Exposes — Before an Attacker Shows You

AI Penetration Testing

Your business is adopting AI faster than your security program can keep up. Chatbots, copilots, and AI agents are now wired into your data, your customers, and your internal systems — and every one of them is a new door an attacker can try to open. Most of these doors were never tested.

www.infosightinc.com info@infosightinc.com 305-828-1003

AI-ACCELERATED. EXPERT-VALIDATED.

We use AI the way elite offensive security teams do — to analyze more data, correlate exploit paths faster, and surface patterns a human alone would take days to find. AI never makes the call. Every exploit chain, privilege escalation, and business-impact finding is executed, verified, and documented by experts — so you get results that are faster than a manual-only test and more trustworthy than a fully automated one.

If you USE AI

Chatbots & customer copilots, Microsoft 365 Copilot & Entra ID, AI features in SaaS you bought, and shadow AI employees adopt on their own.

If you BUILD AI

Custom LLM apps & APIs, retrieval (RAG) pipelines, AI agents with system access, and model gateways and tool integrations.

What We Validate

- Prompt Injection & Jailbreak Resilience
- AI Agent Abuse & Autonomous Actions
- Retrieval (RAG) Data Exposure
- Sensitive Data & PII Leakage
- Identity & Privilege Escalation
- Model & API Security
- Plugin, Tool & Third-Party Integration Risk
- Induced Actions & Real-World Business Impact

An InfoSight AI Penetration Test answers the question your board is already asking:

"Can our AI be tricked, leaked, or turned against us — and how would we know?"

www.infosightinc.com info@infosightinc.com 305-828-1003 InfoSight® www.infosightinc.com

HOW THE ENGAGEMENT WORKS

A structured, end-to-end engagement to identify AI exposure, validate real attack paths, and deliver actionable remediation.

1	**Scope & Threat Modeling**	We map your AI ecosystem, assets and data flows; define business priorities; and model threat actors and attack paths that matter most.
2	**Discovery**	We identify AI tools, integrations, data flows, and permissions including shadow AI and third-party services across the environment.
3	**Exploitation & Validation**	Certified practitioners simulate real-world attacks, exploit findings safely, and validate impact with hands-on testing and abuse-case scenarios.
4	**Risk Scoring**	Findings are ranked by likelihood, impact and business criticality and mapped to frameworks (e.g., NIST AI RMF, OWASP, ISO, SOC 2) so teams know what matters first.
5	**Reporting & Readout**	You receive an executive summary, technical report, prioritized remediation roadmap, and a live walk-through with clear next steps and ownership recommendations.

WHY EXPERT VALIDATION MATTERS

Scanner output

AI-only scanners flag noise and false positives, carry limited business or compliance context, and can't chain realistic multi-step attacks or catch logic and privilege abuse.

InfoSight expert-validated

InfoSight pairs AI-accelerated discovery with human validation: every material finding is confirmed by a certified practitioner, mapped to business impact and relevant regulations, and delivered as a clear, prioritized remediation roadmap — leadership-ready and developer-ready.

FROM RECON TO REMEDIATION VALIDATION POWERED BY MITIGATOR

CYBER RISK AND THREAT INTELLIGENCE PLATFORM

Most penetration test findings live and die in a PDF - read once, filed away, stale the moment the ink dries. InfoSight's don't. Every AI Penetration Testing engagement runs through Mitigator, InfoSight's proprietary threat-intelligence dashboard, and stays there for as long as you're a client.

- A live portal, not a static report - see current AI risk posture any time, no waiting on the next PDF.
- Remediation tracking, not a findings list - every finding carries a status: open, in progress, validated closed.
- Trending over time, not a snapshot - see whether AI risk is going up or down release over release.
- Board-ready views on demand - pull a current risk summary ahead of a board meeting or audit.
- Exposure mapped to your frameworks - NIST AI RMF, OWASP Top 10 for LLMs, HIPAA, PCI DSS, GLBA - updated as findings are remediated.

Ready to see what your AI exposes? Book a scoping call with our AI Pentest experts.