InfoSight
www.infosightinc.com

AI-Accelerated. Expert-Validated.

Penetration Testing

Validate Your Security Before Attackers Compromise It

Real adversaries now use AI to move faster. Your penetration test should too — without ever losing the human judgment that makes findings trustworthy.

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

WHY TRADITIONAL DEFENSES FAIL

Today's adversaries combine AI-accelerated reconnaissance with human ingenuity to find and chain weaknesses faster than static defenses can react. Automated scanners flag noise — they don't think like an attacker, and they can't replicate the judgment of an experienced human operator. Most organizations lack the resources to continuously test these blind spots across network, cloud, application, and OT environments — until someone weaponizes them. That's where InfoSight's Penetration Testing program comes in

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.

INTELLIGENCE-LED SIMULATION

We begin by identifying feasible attack vectors — logical, social, and physical — and test how low-effort vulnerabilities can be chained for deeper compromise. AI accelerates the early, data-heavy phases; certified testers own everything that touches your environment.

1. **Attack Surface Identification:** Prioritize targets within scope, using AI-assisted mapping to cover more ground, faster.
2. **Data Exfiltration Simulation:** Test how far an intruder can go undetected gathering data.
3. **Exploitation & Proof:** Deliver written and video evidence of success.
4. **Vulnerability Assessment:** Identify exploitable weaknesses and correlate them againstrealworld exploitintelligence.
5. **Detection & Incident Response Testing:** Evaluate your visibility and response capabilities.
6. **Access & Escalation:** Simulate lateral movement and privilege abuse — handexecuted by certified testers.

TAILORED TESTING SERVICES BUILT FOR YOUR ENVIRONMENT

Vulnerability & Penetration Testing: Multi-faceted review of external and internal systems, identifying and exploiting vulnerabilities as a real attacker would.

Red Team / Blue Team Exercises: Validate your detection and response readiness. Red teams attack, blue teams defend — revealing gaps in people, process, and technology.

Web, Mobile, API & IAM Security Testing: Evaluate application-layer controls, detect privilege escalation and authorization flaws, and deliver detailed remediation roadmaps.

WHY ENTERPRISES CHOOSE INFOSIGHT

✓ **Real-World Simulation:** Tests go beyond automated scans to mimic live adversaries using exploit chains.	✓ **Business-Aligned Reporting:** Technical and executive reports map vulnerabilities to operational and financial risk.
✓ **AI-Accelerated, Human-Validated:** We use AI to move faster — reconnaissance, correlation, and pattern-matching at scale — but every exploit is executed and verified by a certified human tester. AI accelerates discovery; it never owns the finding.	✓ **Continuous Improvement:** Our methodology supports ongoing testing, rescans, and measurable improvement cycles.
✓ **Proof of Exploit:** Written and video evidence validates findings and supports internal budget and audit justification.	✓ **Experience You Can Trust:** Backed by 25+ years of adversarial testing and regulatory expertise across industries.

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 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 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.

Turn unknown risks into measurable outcomes—schedule your Cybersecurity Risk Assessment today

TAKE THE NEXT STEP

Expose the Gaps Before Adversaries Do—Schedule Your Penetration Test Today