InfoSight
www.infosightinc.com

Stop Assuming Your Firewall Has You Covered

Web Application Testing

Modern attacks don't start at the firewall.
They start in your code, your client-side scripts, your supply chain, and your mis-modeled business logic. Broken access control, insecure design, and poisoned dependencies now drive the majority of impactful breaches—not classic perimeter exploits. InfoSight's Web Application program is built to expose the real exploit paths attackers use today and give your teams exact, prioritized actions to shut them down. Not theoretical risk. Not checkbox scans. Executable evidence.

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

WHERE YOU'RE ACTUALLY EXPOSED NOW

Attack surface has shifted. Most programs haven't.

Core failure points:

- **Access Control & Session Drift:** Role creep, broken object-level authorization, weak session handling, and "just add another flag" logic let attackers move laterally through accounts, tenants, and environments without touching a CVE.
- **Client-Side & Supply Chain Blindness:** Third-party scripts, tag managers, pixels, and open-source packages ship straight to your users' browsers. Compromise one dependency and attackers skim credentials, PII, and payment data at scale.
- **Cloud & Identity Misconfigurations:** Over-privileged service accounts, mis-scoped tokens, SSRF paths to metadata services, and weak secret handling bridge your apps into your cloud core.
- **AI-Speed Offense:** AI-generated phishing, automated recon, fuzzing, and exploit generation compress dwell time and overwhelm manual reviews and legacy testing cycles.

Boards, regulators, and customers now expect proof of control effectiveness, secure-by-design practices, and incident-readiness—not promises.

Proof That Your App Security Actually Works

Security testing either changes attacker options or it is wasted spend.

Effective programs:

- Map tests to real user journeys, abuse cases, and business logic—not generic checklists.
- Validate exploit chains end-to-end: request/response evidence, screenshots, traces, and PoC payloads.
- Prioritize by impact on critical functions, data, and regulatory exposure—not CVSS alone.
- Integrate findings into SDLC so issues stop reappearing in every release.
- Deliver executive-ready narratives that quantify risk reduction, not scan volume.

This is the standard InfoSight designs for. Anything less is noise.

EMBEDDED ACROSS YOUR SOFTWARE DEVELOPMENT LIFE CYCLE

Security embedded at each stage so risk is designed out, not bolted on.



Design & Develop: Threat modeling for critical journeys and role models. Patterns for secure-by-design architectures and zero-trust access to sensitive functions.

Test & Implement: Pre-production assessments tied to release criteria. No promotion of critical apps without proof that key controls work in real attack scenarios.

Maintain & Evolve: Continuous and periodic testing aligned to regulatory and customer obligations. Regression checks ensure new features, integrations, and third-party components do not erode security maturity.

OUR METHODOLOGY

- ✓ **Start from real attacker behaviors and sector-specific threats.**
- ✓ **Quantify how each finding changes attacker options against your business.**
- ✓ **Reframe assumptions about what is "covered" by controls and tools.**
- ✓ **Drive concrete design, code, and process changes that hold under current and emerging threats.**

Full-Stack Application Security Validation

1 Web Attack Surface Testing

Goal-driven testing for web apps and microservices aligned to OWASP Top 10 Security risks.

Focus: broken access control, business logic abuse, data exposure, injection, session and token flaws, rate-limit bypass, misconfigurations.

Output: validated exploit scenarios, mapped to your architecture and owners, with clear remediation paths.

2 Web Security Assessments

Security testing of web and software interfaces to expose:

- Privilege escalation and authorization creep
- Control bypass across environments and tenants
- Flawed flows in registration, password reset, payments, approvals
- Includes a concise, technical report and developer-ready fixes.

3 Vulnerability & Penetration Testing (Application-Led)

Targeted manual penetration testing that mirrors real adversary behavior against your applications and supporting infrastructure.

- External and internal attack paths
- Lateral movement potential via app-layer flaws
- Validation of existing WAF/IPS/EDR controls against real-world techniques

4 Red Team / Blue Team Exercises

Controlled campaigns to test your ability to detect and respond to application-centric attacks.

- Red team: pivots through apps, SSO, and federations to prove impact
- Blue team: measured on visibility, alert quality, investigation depth, and containment
- Result: a measured readiness score and concrete uplift actions.

MITIGATOR®
CYBER RISK AND THREAT INTELLIGENCE PLATFORM

All results are delivered via our Mitigator™ Cyber Risk & Threat Intelligence Platform, with customizable exports for executives, auditors, and regulators.

TAKE THE NEXT STEP

Turn hidden application flaws into verified fixes—schedule your Web Application Security Testing today.