InfoSight
www.infosightinc.com

API SECURITY TESTING

Teach, Tailor, Take Control

☎ 305-828-1003
✉ info@infosightinc.com

Outcome, not checkbox testing.
The assessment is designed to expose how attackers actually traverse your APIs—across mobile, web, partner, and AI integrations—and to give your teams a prioritized plan to remove those paths.

THE MOST DIRECT PATH INTO YOUR BUSINESS

Modern applications run on interconnected services, open-source components, and third-party integrations, which means one weak endpoint, leaked key, or misconfigured control can expose everything behind it. Attackers target APIs to exploit business logic, pivot through integrations, and exfiltrate sensitive data at scale.

WHY THIS SHOULD WORRY YOU

Traditional app testing misses where APIs actually break: authorization, token handling, data exposure, and integration points. The result is an expanding attack surface with limited evidence of how real-world threats would move through it.

HOW WE EXPOSE THE GAPS

Our API Security Assessment is a threat-led, standards-aligned review of your API ecosystem. We map your true attack surface, validate controls against current attack patterns, and pressure-test high-value workflows instead of running generic scans.

WHAT WE PUT IN YOUR HANDS

Actionable, prioritized findings with proof-of-exploit and clear remediation steps your internal teams and partners can implement fast, tightening API security with every release.

BOARDS, REGULATORS, AND CUSTOMERS NOW EXPECT EVIDENCE THAT YOUR APIS ARE SECURE BY DESIGN—HARDENED AUTHENTICATION, LEAST-PRIVILEGE ACCESS, ABUSE-RESISTANT LOGIC, AND TESTED INCIDENT PLAYBOOKS—NOT ASSURANCES.

THE API SECURITY ASSESSMENT IS A FOCUSED, MULTI-DISCIPLINARY ENGAGEMENT THAT:

- Identifies and maps your real API attack surface
- Simulates modern attacker techniques against that surface
- Validates your ability to detect and respond
- Delivers a clear, ordered plan to close the gaps—backed by evidence, not assumptions

OUR API SECURITY ASSESSMENT:

1. Web Attack Surface Testing

- Full API inventory across documented, shadow, and legacy endpoints
- Mapping of auth flows, tokens, scopes, roles, and trust relationships
- Identification of high-value data flows and business-critical operations
- Alignment to OWASP API Security Top 10 (2023) with real environment context

2. Threat-Led Testing (Not Generic Scans)

- Abuse-case driven testing based on how real attackers monetize your APIs:
  - BOLA/BOPLA and broken function-level authorization
  - Broken authentication and token handling
  - Injection attacks across REST, GraphQL, gRPC, and microservices
  - Insecure direct object references, mass assignment, and excessive data exposure
  - Misconfigurations: CORS, TLS, rate limits, error handling, management endpoints
- Targeted exploitation to prove impact without operational disruption.

3. Supply Chain, AI, and Integration Focus

- Assessment of third-party and AI/LLM-integrated APIs that handle identity, payments, PHI/PII, or control functions
- Review of secrets management, CI/CD exposure, and vendor API hygiene
- Validation that partner and plugin APIs cannot pivot into core systems.

4. Human Layer and Operations (Optional Add-Ons)

To complete the attack-path view:

- Red Team / Blue Team Exercises
- Simulated campaigns using API-centric attack paths to test detection, response, and escalation across SOC, DevOps, and AppSec.
- Social Engineering
- Targeted pretexts aligned to developer and admin workflows to expose process gaps that put API keys, tokens, and credentials at risk.

Mitigator-Delivered Reporting and Continuous Validation

MITIGATOR®
VULNERABILITY & THREAT MANAGER

All findings and workflows are delivered through the Mitigator Vulnerability & Threat Management Platform:

Exploit-path evidence: requests, traces, and proof-of-impact that development and security teams can reproduce

Prioritized remediation by attacker options removed, not raw CVSS scores

Executive summary that links API exposures to business processes, customers, and regulatory impact

Tracking of remediation status and retest results to prove risk reduction over time

Support for recurring and on-demand retesting cycles to match your release velocity

TAKE THE NEXT STEP

Turn hidden API exposures into verified fixes—schedule your API Security Assessment now.