InfoSight
www.infosightinc.com



App Store Validation Is Not an Enterprise Security Control

Mobile App Security Testing

Attackers do not care that your app "passed review."
They target weak mobile logic, lost devices, third-party SDKs, insecure push, and unprotected data at rest. Mobile is now a primary path to account takeover, fraud, and regulatory exposure—not a side project. InfoSight's Mobile Application Security Testing is built to break the assumptions your team is relying on and prove exactly how your iOS and Android apps can be abused in the real world—then give your developers merge-ready fixes.

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

THE REAL ATTACK SURFACE BEHIND YOUR MOBILE APP

Headline issues that legacy testing and basic scans miss:

- **Abuse of Legitimate Functionality:** Weak authorization, broken deep links, business logic flaws, insecure redirects, and "convenience" shortcuts that allow privilege escalation without a traditional exploit.
- **Device and Data Exposure:** Credentials, tokens, keys, and PII stored in plaintext, logs, screenshots, or insecure local databases. Lost, stolen, or rooted devices turn into instant data disclosure.
- **Third-Party SDK & Supply Chain Risk:** Advertising, analytics, social login, and push SDKs drag in CVEs, over-permissive scopes, and data exfil paths your team never reviews.
- **Weak Encryption & Broken TLS:** Improper certificate validation, poor key management, and downgraded protocols give attackers a clear line into "encrypted" sessions.
- **Push & Session Hijacking:** Improper token binding, replayable sessions, and insecure notification flows open the door to account takeover and transaction manipulation.

WHAT EFFECTIVE MOBILE APP SECURITY DELIVERS

Non-negotiables for a modern mobile security program:

- Verified protection of authentication, authorization, and sessions against real attacker techniques.
- Clean separation between mobile client and backend trust; no sensitive logic or secrets exposed on the device.
- Full inventory and validation of third-party SDKs and libraries.
- Encryption, key handling, and certificate validation that hold up against rooted/jailbroken devices and active network attackers.
- Reporting that development, security, compliance, and the board can all act on—without translation.

THREAT-LED, EXPLOIT-VALIDATED, DEVELOPER-READY.

1

Threat Modeling & Architecture Review

Map how your app really works: data flows, auth flows, deep links, jailbreak/root exposure, certificate pinning, storage behaviors. Aligns testing to high-impact abuse cases, not generic checklists.

2

Static Code Review (SAST)

Source and binary analysis to identify:

- Hardcoded secrets and credentials
- Insecure crypto and randomization
- Unsafe debug settings and logging
- Broken input validation and error handling

3

Dynamic Analysis (DAST) on Real Devices

Instrumented, rooted/jailbroken device testing to validate:

- Insecure storage (SQLite, plist, shared prefs, keychain misuse)
- TLS weaknesses and SSL pinning bypasses
- Session fixation, token theft, replay attacks
- Input tampering and parameter manipulation

4

Manual Exploitation & Abuse Testing

Experienced testers chain findings into real attack paths:

- Account and role escalation
- Unauthorized data access
- Transaction tampering and workflow bypass
- Outputs are exploit-path narratives, not just CVE lists.

5

Third-Party SDK & Supply Chain Assessment

Inventory and validate all embedded SDKs, libraries, and services:

- Known vulnerabilities and misconfigurations
- Data sharing behavior vs policy and regulation
- Over-privileged permissions and risky domains

6

Secure SDLC & Store-Readiness Guidance

Concrete guidance mapped to OWASP MASVS and OWASP Mobile Top 10, supporting:

- App Store / Play Store security expectations
- Regulated environments (financial services, healthcare, government, etc.)
- CI/CD pipeline checks to prevent regressions

7

Continuous, On-Demand Mobile VMaaS

Annual model designed for frequent updates:

- Unlimited or high-frequency retesting of new builds within the service term
- Rapid verification of hotfixes and feature updates against the same threat model and scenarios
- Always-current assurance instead of point-in-time certification

EMBEDDED ACROSS THE MOBILE SDLC

Security is wired into how you build and ship, not stapled on at release.

Design & Develop

Threat models and security requirements for authentication, roles, data flows, and offline behavior. Baseline patterns for secure storage, and encryption.

Test & Release

Mobile security testing as a release gate for major versions and high-risk features. No production launch without evidence that critical controls hold.

Maintain & Evolve

Periodic re-testing for new builds, frameworks, and SDK changes. Continuous validation that updates, hotfixes, and dependencies have not reopened old paths.



MITIGATOR®
CYBER RISK AND THREAT INTELLIGENCE PLATFORM

All results are delivered via our Mitigator™ Cyber Risk & Threat Intelligence Platform, a single portal to see exposures across your mobile apps and connected services with customizable exports for executives, auditors, and regulators.

TAKE THE NEXT STEP

Turn hidden mobile app risks into verified fixes—schedule your Mobile Application Security Testing today.