SECURITY INNOVATION

MOBILE

DEVELOP DEFENSES AGAINST MOBILE THREATS

As organizations struggle with the nuances of mobile platforms, development teams often create applications that are not designed or coded to withstand the unique threats associated with mobile environments. Developers often make flawed assumptions like trusting the mobile client or server connection – mistakes that allow an attacker to bypass protections or masquerade as a legitimate service.

Security Innovation offers a suite of solutions that helps organizations assess risk and improve mobile security from multiple perspectives – external attackers, malicious internal users, and even unintentioned employees.

MOBILE CENTERS OF EXCELLENCE (COE)

Our Mobile Center of Excellence conducts ongoing research on all popular platforms (Android, iOS, Windows Mobile, Blackberry), technologies, and commonly used hardware components. This yields continual skills progression, methodology refinement, and tools development that allow us to conduct specialized testing and provide informed remediation advice and education solutions for our clients.

MOBILE SECURITY TRAINING

Build security into mobile applications and staff culture

Security Innovation offers 120+ computer-based and instructor-led training courses that cover secure development and staff awareness. Popular Mobile courses include:

- Mobile Device Security
- Secure Mobile Development Fundamentals
- Fundamentals of Mobile Development - Embedded
- Creating Secure Code - iPhone
- Creating Secure Code - Android
- Creating Secure iPhone Code - Objective-C

MOBILE SECURITY ASSESSMENTS

We don't just find vulnerabilities, we help remediate them

For more than a decade, organizations have relied on our engineers to conduct complex attacks on software, devices, and back-end systems with the same level of sophistication and determination that an attacker would. This is complement by internally developed tools and specialized products to conduct deep and targeted analysis that includes:

- Simulating real-world OS and application-level attacks
- Threat modeling to identify risks, cover multiple abuse cases, and guide test planning
- Penetration testing and code review to find and mitigate specific vulnerabilities

For each vulnerability found, we assign a risk rating specific to your environment, describe the business impact, document steps to reproduce, and provide prescriptive remediation guidance (including code samples) for your specific mobile platform.

STANDARDS & PROCESS

Adopt secure mobile development best practices

Security Innovation's Secure Coding Knowledgeable and comprehensive inspection of your Software Development Lifecycle can allow organizations to adopt key best practices in order to better facilitate secure mobile application development.

SECURE CODING KNOWLEDGEBASE

- 2,500 searchable how-to's, checklists, code samples, principles and other guidance assets
- Dedicated guidance (150+ articles) for Android and iPhone using ObjectiveC, Java, and C++
- Complete team guidance for architects, developers, test/QA, program management, etc.

SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) OPTIMIZATION

- Analyzes your existing SDLC against OWASP Mobile Top Ten, ISO, NIST, and PCI DSS
- Identifies and fills gaps with proper training, activities, and tools usage
- Creates a roadmap that includes detailed recommendations and optimal sequencing