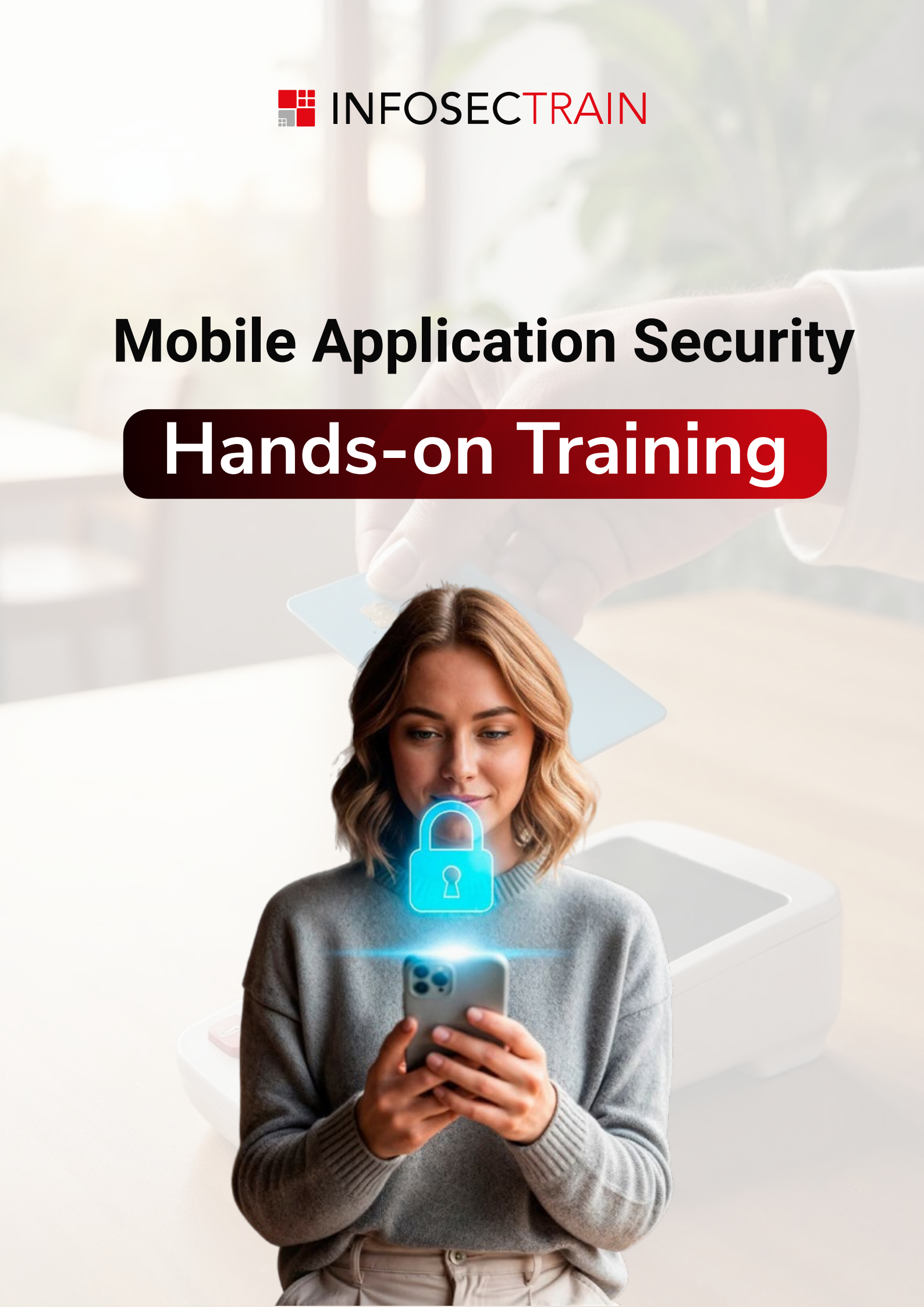
INFOSECTRAIN

Mobile Application Security

Hands-on Training



INFOSECTRAIN

Course Highlights

- **40-Hour LIVE** Instructor-Led Training
- Hands-on 15+ Security Tools
- Telegram Group for Exam Support
- Real-World Case Studies
- Android & iOS Coverage
- Certified Experts
- OWASP & MASVS Focus
- Access to Recorded Sessions
- Career Guidance & Mentorship

INFOSECTRAIN

About Course

With the exponential growth of mobile apps, security has become a top priority for organizations. This course provides a comprehensive learning path covering mobile app architectures, OWASP Mobile Top 10, penetration testing methodologies, and advanced tools for static and dynamic analysis. You'll explore real-world attack vectors, reverse engineering, obfuscation, and Mobile Application Security Verification Standard (MASVS). By the end, you'll have the expertise to perform professional mobile app security assessments.

INFOSECTRAIN

Course Objectives

Upon successful completion of the training, participants will be able to:

- Understand the fundamentals of mobile application security and architecture.
- Conduct penetration testing on Android and iOS applications.
- Apply OWASP Mobile Top 10 and MASVS frameworks in real-world testing.
- Use advanced tools like Frida, MobSF, Burp, Objection for security assessments.
- Perform static and dynamic analysis of apps including reverse engineering.

INFOSECTRAIN

Target Audience

The training is ideal for:

- Security Professionals & Penetration Testers
- Application Developers (iOS & Android)
- QA & Security Test Engineers
- IT Administrators & Security Architects
- Cybersecurity Students & Enthusiasts

Pre-requisites

- Web & API Pen Testing Basics
  - Understand HTTP/S, headers, cookies, sessions
  - Familiarity with OWASP Top 10 (especially for APIs)
  - Experience with tools like Burp Suite, Postman, and curl
- Mobile OS Fundamentals
  - Know how Android and iOS differ in architecture
  - Understand app lifecycle, permissions, and sandboxing
  - Be able to navigate settings, install APKs/IPAs, and use emulators

Technical Requirements

- Hardware/Devices
  - iPhone 6s (iOS 15.8 or above)
  - Google Pixel 2 or Pixel 3 (Android)
  - Data cable Type-A to Lightning

INFOSECTRAIN

Course Content

Module 1: Introduction to Mobile Applications & Security

- Evolution of Mobile Applications
- Importance of Mobile Application Security
- Key Threats in Mobile Ecosystems

Module 2: Fundamentals of Penetration Testing

- Penetration Testing Process
- Penetration Testing Methodologies
- Mobile Application Security Standards

Module 3: Mobile Platform Attack Vectors

- Top 10 Risks for Mobile Devices
- Attacking Vectors & Vulnerabilities
- Case Studies: Agent Smith, SS7, Simjacking

Module 4: Mobile Device Management (MDM) & Security

- MDM Models
- Mobile Access Control System
- Remote Wipe Mechanisms
- Understanding Miradore

Module 5: OWASP Mobile Top 10 Risks

- M1: Improper Credential Usage
- M2: Inadequate Supply Chain Security
- M3: Insecure Authentication/Authorization
- M4: Insufficient Input/Output Validation
- M5: Insecure Communication
- M6: Inadequate Privacy Controls
- M7: Insufficient Binary Protections
- M8: Security Misconfiguration
- M9: Insecure Data Storage
- M10: Insufficient Cryptography

Module 6: Setting Up Mobile Devices for Testing

- Preparing Android & iOS Devices
- Installing Required Tools (ADB, Cydia Impactor, etc.)
- Bypassing Business Logic for Exploitation

Module 7: Mobile Application Security Tools

- Overview & Hands-On with Tools:

  MobSF, Drozer, Frida, ADB, APPIE

  jdGUI, Dex2Jar, Burp, Charles Proxy

  Cydia Impactor, GDB, Objection

Module 8: Static Application Analysis

- Retrieving iOS & Android Apps for Reverse Engineering
- Decompiling Android Applications
- Circumventing iOS App Encryption
- Accelerating iOS Disassembly: Hopper & IDA Pro
- Android Application Analysis with MobSF

Module 9: Reverse Engineering Obfuscated Applications

- Identifying Obfuscation Techniques
- Decompiling Obfuscated Applications
- Decrypting Obfuscated Content with Simplify

Module 10: Dynamic Application Analysis

A. Manipulating & Analyzing iOS Applications

- Runtime iOS Application Manipulation with Cycript & Frida
- Method Swizzling in iOS
- iOS Application Vulnerability Analysis with Objection
- Tracing iOS Application Behavior & API Use
- Extracting Secrets with KeychainDumper
- Method Hooking with Frida & Objection

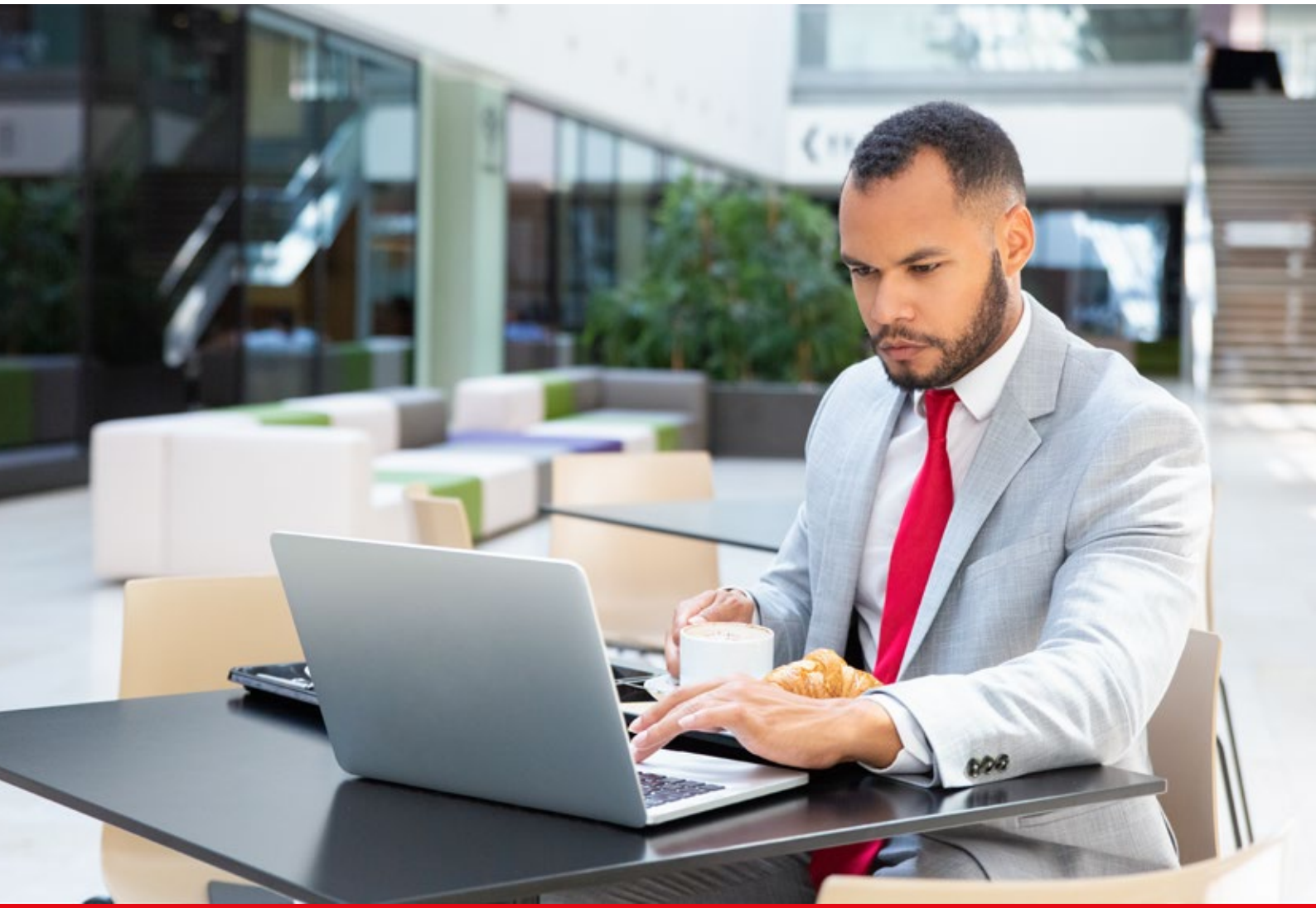
B. Manipulating & Analyzing Android Applications

- Android Application Manipulation with Apktool
- Reading & Modifying Dalvik Bytecode
- Adding Android Application Functionality (Java to Dalvik)
- Method Hooking with Frida & Objection

Module 11: Mobile Application Security Verification Standard (MASVS)

- Step-by-Step Recommendations for Application Analysis
- Methodical Approach to Security Verification
- Common Pitfalls in Application Security Assessments

INFOSECTRAIN
Educate. Excel. Empower.



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on