Securing CI/CD for Mobile Applications Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern enterprise is fundamentally mobile, and the velocity of release demanded by today's market is achieved through Continuous Integration/Continuous Delivery pipelines. However, this speed often comes at the expense of robust security, creating a critical gap in the Software Development Life Cycle. Securing CI/CD for Mobile Applications Training Course addresses the Shift-Left imperative, moving security practices from late-stage testing to the earliest phases of code commit and automated build. It is designed to equip Development, Operations, and Security teams with the practical, DevSecOps skills necessary to automate security gates and vulnerability detection within the mobile CI/CD workflow, ensuring rapid delivery does not compromise app integrity or expose sensitive user data and intellectual property.

This intensive course will focus on the unique security challenges of iOS and Android ecosystems including code signing, secrets management, and software supply chain risks as they manifest within automated pipelines. Participants will master SAST, DAST, and IAST tool integration, learn to establish non-negotiable security policies that halt vulnerable builds, and implement secure configuration best practices for CI/CD infrastructure. By the end of the program, attendees will be able to design, implement, and maintain a truly secure and resilient mobile CI/CD pipeline, transforming security from a bottleneck into an accelerator for delivering high-quality, trustworthy mobile applications at scale.

Programme Curriculum

Securing CI/CD for Mobile Applications Training Course

Introduction

The modern enterprise is fundamentally mobile, and the velocity of release demanded by today's market is achieved through Continuous Integration/Continuous Delivery pipelines. However, this speed often comes at the expense of robust security, creating a critical gap in the Software Development Life Cycle. Securing CI/CD

for Mobile Applications Training Course addresses the Shift-Left imperative, moving security practices from late-stage testing to the earliest phases of code commit and automated build. It is designed to equip Development, Operations, and Security teams with the practical, DevSecOps skills necessary to automate security gates and vulnerability detection within the mobile CI/CD workflow, ensuring rapid delivery does not compromise app integrity or expose sensitive user data and intellectual property.

This intensive course will focus on the unique security challenges of iOS and Android ecosystems including code signing, secrets management, and software supply chain risks as they manifest within automated pipelines. Participants will master SAST, DAST, and IAST tool integration, learn to establish non-negotiable security policies that halt vulnerable builds, and implement secure configuration best practices for CI/CD infrastructure. By the end of the program, attendees will be able to design, implement, and maintain a truly secure and resilient mobile CI/CD pipeline, transforming security from a bottleneck into an accelerator for delivering high-quality, trustworthy mobile applications at scale.

Course Duration

5 days

Course Objectives

1. Integrate security best practices into all stages of the CI/CD pipeline, effectively adopting a Shift-Left strategy.
2. Securely configure CI/CD tools to prevent unauthorized access and pipeline manipulation.
3. Implement robust secrets management solutions to eliminate hardcoded credentials from source code and environments.
4. Automate Static (SAST) and Dynamic Application Security Testing for both iOS and Android apps in the CI/CD flow.
5. Enforce secure coding standards and perform dependency scanning to mitigate risks from open-source libraries and transitive dependencies.
6. Identify and remediate OWASP Mobile Top 10 vulnerabilities within the context of a continuous delivery environment.
7. Implement best practices for mobile code signing certificate and provisioning profile security and rotation.
8. Scan and validate secure configuration of infrastructure templates used in deployment.
9. Integrate Mobile App Protection (MAP) / In-App Protection tools for runtime self-protection (RASP) during the build process.
10. Design and deploy automated "Break the Build" security policies based on severity thresholds and compliance checks.
11. Defend against software supply chain attacks by verifying build artifacts and controlling third-party component usage.
12. Establish continuous security monitoring and detailed audit logging across the entire CI/CD and deployment environment.
13. Conduct targeted threat modeling specific to the mobile application's CI/CD process to proactively identify high-impact risks.

Target Audience

1. DevOps Engineers & DevSecOps Engineers
2. Mobile Application Developers
3. Security Architects & Application Security Analysts
4. Cloud Engineers involved in mobile pipeline infrastructure

5. Quality Assurance (QA) Engineers & Automation Testers
6. Technical Project Managers overseeing mobile releases
7. Release Managers responsible for deployment velocity and integrity
8. Penetration Testers seeking to improve collaboration and "shift-left" testing

Course Modules

Module 1: DevSecOps & Mobile CI/CD Fundamentals

- Principles of DevSecOps and the Shift-Left philosophy in mobile development.
- Overview of the Mobile CI/CD Pipeline architecture.
- Unique security challenges for iOS and Android
- Threat Modeling the mobile CI/CD pipeline and identifying high-risk stages.
- Integrating security checks without impacting deployment velocity.
- Case Study: Analyzing a popular app's unauthorized app store submission due to weak pipeline access controls.

Module 2: Secure Code & Dependency Scanning (SAST)

- Implementing Static Application Security Testing early via pre-commit hooks and build steps.
- Scanning for mobile-specific vulnerabilities
- Managing vulnerable dependencies using Software Composition Analysis tools.
- Automating reporting and ticketing for SAST findings into developer workflows
- Configuring Code Quality Gates to fail the build on high-severity SAST findings.
- Case Study: A breach caused by an outdated, vulnerable third-party library dependency being pulled into the CI build.

Module 3: Dynamic Analysis and Security Testing (DAST/IAST)

- Integrating Dynamic Application Security Testing in a pre-production/staging environment.
- Using Interactive Application Security Testing to bridge the gap between SAST and DAST.
- Automating API Security Testing for mobile backend communication and exposed endpoints.
- Leveraging Mobile Emulators/Device Farms to run DAST scans consistently and at scale.
- Analyzing DAST reports and establishing efficient vulnerability triage processes.
- Case Study: A failure to detect an API endpoint vulnerability accessible through an authenticated DAST scan, leading to a production data leak.

Module 4: Secrets Management & Hardening CI/CD Infrastructure

- Best practices for Secrets Management using vaults
- Securely injecting secrets as environment variables only at runtime during the build/deployment.
- Hardening CI/CD servers.
- Using containerized build environments for build isolation and security.
- Implementing and rotating Role-Based Access Control for CI/CD user accounts.
- Case Study: The exploitation of a CI server misconfiguration that allowed an attacker to retrieve all stored deployment credentials.

Module 5: Mobile Artifact Security

- Securing and automating the use of iOS/Android code signing assets
- Protecting the final build artifact from tampering post-build.
- Integrating Mobile App Protection / App Hardening tools into the build step.

- Implementing anti-tampering and anti-reverse-engineering controls.
- Verifying the integrity and authenticity of the build artifact before deployment/distribution.
- Case Study: A scenario where a legitimate app was repackaged and signed with a compromised developer key due to poor key management.

Module 6: Infrastructure as Code (IaC) and Configuration Security

- Introduction to IaC security scanning tools for pipeline configuration files.
- Scanning Cloud Configuration templates used by the CI/CD for misconfigurations.
- Defining and enforcing security baselines and compliance policies for build environments.
- Using security-focused base images for containerized CI/CD agents.
- Auditing and securing the configuration-as-code repository
- Case Study: A cloud infrastructure misconfiguration introduced via an insecure Terraform script that exposed a build artifact storage bucket.

Module 7: Software Supply Chain Defense

- Third-party component vulnerabilities and repo poisoning.
- Implementing provenance tracking and artifact verification
- Securely managing and restricting external dependencies and package sources.
- Using Notary services or similar tools for digital signing of artifacts across the pipeline.
- Mitigating the risk of compromised build agents or injection attacks.
- Case Study: A large-scale software supply chain attack and how similar vulnerabilities could impact a mobile CI/CD setup.

Module 8: Continuous Security Monitoring & Remediation

- Setting up Continuous Security Monitoring and alerting on pipeline anomalies.
- Integrating security metrics into the DevSecOps dashboard
- Establishing a rapid and actionable security feedback loop for developers.
- Automating incident response and rollback procedures for failed security gates.
- Security logging best practices for auditing all pipeline activities and access attempts.
- Case Study: An analysis of a continuous monitoring system detecting an unusual deployment activity outside of business hours, triggering an automatic build-halt.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com