Integrating Security into CI/CD Pipelines 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 rapid acceleration of software delivery, driven by Continuous Integration (CI) and Continuous Delivery (CD) practices, has necessitated a paradigm shift in application security. Traditional security approaches, which introduce checks at the end of the Software Development Life Cycle (SDLC), are simply too slow and inefficient for modern DevOps environments. This course addresses that critical gap by fully immersing participants in the principles and practices of DevSecOps. We will focus on the essential "shift-left" methodology, ensuring that security policies, automated security testing, and vulnerability remediation are embedded seamlessly from the initial code commit through to production deployment. You will gain practical, hands-on experience using industry-leading Application Security Tools to build and maintain secure, auditable, and compliant CI/CD pipelines, directly reducing security risk and time-to-market.

Integrating Security into CI/CD Pipelines Training Course is designed to transform developers, operations staff, and security professionals into DevSecOps champions. You'll master the automation of crucial security functions like Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), and Secrets Management. The training emphasizes building secure-by-design and cloud-native applications by implementing security gates and policy-as-code to prevent misconfigurations, manage open-source dependencies, and safeguard critical infrastructure as code (IaC). By the end of this course, you will possess the practical skills to harden any CI/CD pipeline, fostering a culture of shared security responsibility across your entire engineering organization.

Programme Curriculum

Integrating Security into CI/CD Pipelines Training Course

Introduction

The rapid acceleration of software delivery, driven by Continuous Integration (CI) and Continuous Delivery (CD) practices, has necessitated a paradigm shift in application security. Traditional security approaches, which introduce checks at the end of the Software Development Life Cycle (SDLC), are simply too slow and inefficient for modern DevOps environments. This course addresses that critical gap by fully immersing participants in the principles and practices of DevSecOps. We will focus on the essential "shift-left" methodology, ensuring that security policies, automated security testing, and vulnerability remediation are embedded seamlessly from the initial code commit through to production deployment. You will gain practical, hands-on experience using industry-leading Application Security Tools to build and maintain secure, auditable, and compliant CI/CD pipelines, directly reducing security risk and time-to-market.

Integrating Security into CI/CD Pipelines Training Course is designed to transform developers, operations staff, and security professionals into DevSecOps champions. You'll master the automation of crucial security functions like Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), and Secrets Management. The training emphasizes building secure-by-design and cloud-native applications by implementing security gates and policy-as-code to prevent misconfigurations, manage open-source dependencies, and safeguard critical infrastructure as code (IaC). By the end of this course, you will possess the practical skills to harden any CI/CD pipeline, fostering a culture of shared security responsibility across your entire engineering organization.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Implement the Shift-Left methodology by integrating security tools into the earliest stages of the SDLC.
2. Foster a collaborative DevSecOps culture and establish security as a shared responsibility.
3. Automate Static Application Security Testing (SAST) in the CI pipeline for immediate code feedback.
4. Implement Software Composition Analysis (SCA) to mitigate software supply chain risk and manage open-source vulnerabilities.
5. Integrate secure Secrets Management solutions to eliminate hardcoded credentials.
6. Configure and execute Dynamic (DAST) and Interactive (IAST) security testing in staging environments.
7. Define and enforce security policies using Policy-as-Code (PaC) frameworks.
8. Secure Infrastructure as Code (IaC) templates using specialized scanning tools.
9. Implement Container Security scanning and vulnerability management for Docker and Kubernetes.
10. Establish and manage automated Security Gates to halt the pipeline upon critical vulnerability detection.
11. Incorporate continuous Threat Modeling into the development workflow for proactive risk identification.
12. Automate compliance checks for standards like GDPR, HIPAA, or PCI-DSS within the pipeline.
13. Design and optimize fast, effective vulnerability remediation workflows with developer-friendly reporting.

Target Audience

1. DevOps Engineers and SREs
2. Application Security Engineers
3. Software Developers and Architects
4. CI/CD Pipeline Owners
5. Cloud Engineers (AWS, Azure, GCP)
6. IT Security Analysts and Consultants
7. Quality Assurance (QA) Engineers specializing in automation

8. Technical Project Managers leading DevSecOps adoption

Course Modules

Module 1: DevSecOps Fundamentals and Culture

- Defining DevSecOps, the Shift-Left imperative, and the integration of security.
- Understanding the CI/CD pipeline stages
- Establishing a Security Champion program and fostering a shared security responsibility culture.
- Introducing the core categories of Application Security Tools
- Mapping security requirements to common regulatory standards
- Case Study: Target Corporation Data Breach.

Module 2: Static Analysis and Secure Coding

- Integrating SAST into the Code Commit and Build stages of the pipeline.
- Configuring SAST rulesets and managing false positives effectively.
- Implementing pre-commit Git Hooks to enforce secure coding standards locally.
- Reviewing the OWASP Top 10 and ensuring checks cover critical vulnerabilities.
- Automating reporting and providing direct, actionable feedback to developers.
- Case Study: Log4j Vulnerability Remediation.

Module 3: Dependency and Software Supply Chain Security

- Implementing Software Composition Analysis to scan third-party libraries and dependencies.
- Understanding and mitigating the risks associated with Open-Source Software.
- Generating a Software Bill of Materials automatically within the build process.
- Setting up policy gates to reject builds with critical or high-severity vulnerabilities.
- Addressing sophisticated threats like Dependency Confusion and repository compromise.
- Case Study: Codecov Supply Chain Attack.

Module 4: Secure Secrets and Configuration Management

- Identifying and eliminating hardcoded credentials from source code and configuration files.
- Integrating a centralized Secrets Management solution into the pipeline.
- Implementing least-privilege access and dynamic secrets for CI/CD runners.
- Securely managing and rotating API keys, tokens, and database credentials.
- Configuring runtime environment variable injection for secure deployment.
- Case Study: Capital One Breach.

Module 5: Infrastructure as Code (IaC) Security

- Scanning IaC templates for misconfigurations and security flaws.
- Enforcing security baselines using Policy-as-Code tools like Open Policy Agent
- Preventing configuration drift between development, staging, and production environments.
- Securing networking, storage, and Identity and Access Management permissions in the IaC pipeline.
- Integrating IaC security scanning as a mandatory check before provisioning.
- Case Study: Tesla AWS Misconfiguration.

Module 6: Container and Image Security

- Scanning container images for operating system and application layer vulnerabilities.

- Implementing policies to prevent the use of insecure or outdated base images.
- Integrating Container Image Scanning into the build and registry phases.
- Securing Kubernetes deployments using admission controllers and security contexts.
- Implementing image signing and Binary Authorization for trusted deployments.
- Case Study: Docker Hub Credentials Leak.

Module 7: Dynamic Testing and Security Gates

- Automating Dynamic Application Security Testing against a running staging environment.
- Using IAST to get real-time vulnerability data during functional and QA testing.
- Setting up an effective Security Gate to automatically block deployment to production based on risk severity.
- Integrating security test results with bug tracking systems for developer workflow.
- Conducting lightweight automated Penetration Testing simulations in the pipeline.
- Case Study: OWASP ZAP in a Financial Services Pipeline.

Module 8: Continuous Monitoring and Advanced DevSecOps

- Implementing Security Observability for continuous monitoring of security events in production.
- Establishing automated feedback loops from production monitoring back to the CI/CD pipeline.
- Exploring advanced topics.
- Integrating API Security testing and GraphQL schema analysis into the pipeline.
- Measuring DevSecOps success: Key metrics, KPIs, and dashboard creation.
- Case Study: Netflix Security Automation.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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