DevSecOps Engineer Certification (ECDE) Training Course

Professional Development Training Course Outline

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

Course Introduction

DevSecOps Engineer Certification (ECDE) Training Course equips IT professionals, software engineers, and security specialists with the knowledge and skills to integrate security seamlessly into the DevOps pipeline. With increasing cyber threats and accelerated software delivery cycles, organizations require engineers who can embed security best practices, automated compliance, and continuous monitoring into development, testing, and deployment processes. This course emphasizes secure coding, threat modeling, vulnerability management, CI/CD pipeline security, container and cloud security, and real-time monitoring, ensuring participants can protect applications without slowing development.

Participants will gain hands-on experience with modern DevSecOps tools, automated security testing frameworks, and best practices for collaboration between development, operations, and security teams. The training covers risk management, compliance frameworks, and security policy enforcement while highlighting emerging trends in cloud-native security, DevOps automation, and regulatory compliance. By the end of this course, participants will be able to implement end-to-end DevSecOps strategies, strengthen organizational security posture, and support continuous, secure software delivery.

Programme Curriculum

DevSecOps Engineer Certification (ECDE) Training Course

Introduction

DevSecOps Engineer Certification (ECDE) Training Course equips IT professionals, software engineers, and security specialists with the knowledge and skills to integrate security seamlessly into the DevOps pipeline. With increasing cyber threats and accelerated software delivery cycles, organizations require engineers who can embed security best practices, automated compliance, and continuous monitoring into development, testing, and deployment processes. This course emphasizes secure coding, threat modeling, vulnerability

management, CI/CD pipeline security, container and cloud security, and real-time monitoring, ensuring participants can protect applications without slowing development.

Participants will gain hands-on experience with modern DevSecOps tools, automated security testing frameworks, and best practices for collaboration between development, operations, and security teams. The training covers risk management, compliance frameworks, and security policy enforcement while highlighting emerging trends in cloud-native security, DevOps automation, and regulatory compliance. By the end of this course, participants will be able to implement end-to-end DevSecOps strategies, strengthen organizational security posture, and support continuous, secure software delivery.

Course Objectives

1. Understand the DevSecOps principles and frameworks for secure software delivery.
2. Integrate security practices into CI/CD pipelines using automation tools.
3. Implement threat modeling and secure coding techniques.
4. Conduct vulnerability scanning, penetration testing, and risk assessments.
5. Manage cloud security, container security, and infrastructure-as-code security.
6. Apply compliance standards and regulatory requirements to software development.
7. Utilize security monitoring and logging for proactive threat detection.
8. Automate security testing in development and deployment processes.
9. Improve collaboration between development, operations, and security teams.
10. Implement incident response and remediation strategies in DevSecOps environments.
11. Measure security metrics and KPIs to drive continuous improvement.
12. Secure software supply chains and third-party dependencies.
13. Develop organizational policies and best practices for DevSecOps adoption.

Organizational Benefits

- Improved software security and reduced vulnerability exposure
- Faster, secure software delivery cycles through automation
- Enhanced compliance with industry standards and regulations
- Strengthened collaboration between Dev, Ops, and Security teams
- Reduced risk of breaches, incidents, and financial losses
- Improved efficiency in security testing and monitoring processes
- Better protection of cloud-native and containerized applications
- Increased staff expertise in modern DevSecOps practices
- Stronger organizational security culture and governance
- Competitive advantage through secure and reliable software delivery

Target Audiences

- Software engineers and developers
- DevOps engineers and infrastructure specialists
- Security analysts and cybersecurity professionals
- IT managers and system administrators
- Cloud and container platform engineers
- Compliance and risk management officers
- Technical architects and solution designers
- Students and professionals pursuing DevSecOps certification

Course Duration: 10 days

Course Modules

Module 1: Introduction to DevSecOps

- Overview of DevSecOps principles and practices
- Understanding the DevOps lifecycle and integration of security
- Security challenges in modern software development
- Roles and responsibilities in a DevSecOps team
- Benefits of embedding security early in development
- Case Study: Successful DevSecOps implementation in a global tech firm

Module 2: Secure Coding & Application Security

- Best practices for secure coding and code reviews
- Common vulnerabilities and how to prevent them (OWASP Top 10)
- Secure design patterns for applications
- Input validation, authentication, and session management
- Threat modeling for proactive security
- Case Study: Reducing critical vulnerabilities in a web application

Module 3: CI/CD Pipeline Security

- Integrating automated security checks into pipelines
- Securing build and deployment stages
- Using tools for static and dynamic code analysis
- Continuous testing for vulnerabilities
- Pipeline monitoring and incident alerts
- Case Study: Automated security testing in CI/CD for an e-commerce platform

Module 4: Vulnerability Management & Risk Assessment

- Scanning tools for detecting vulnerabilities
- Prioritizing and remediating risks
- Conducting penetration testing on applications and infrastructure
- Implementing patch management strategies
- Security risk documentation and reporting
- Case Study: Mitigating high-risk vulnerabilities in a fintech application

Module 5: Cloud & Container Security

- Securing cloud-native applications and services
- Container and orchestration security best practices
- Infrastructure as Code (IaC) security considerations
- Identity and access management for cloud environments
- Network segmentation and secure communications
- Case Study: Securing microservices and container deployments in production

Module 6: Compliance, Policies & Regulatory Requirements

- Mapping compliance standards to DevSecOps practices
- GDPR, HIPAA, PCI-DSS, and other regulations
- Policy enforcement within pipelines and processes

- Documentation and audit trails for compliance
- Governance frameworks for security practices
- Case Study: Aligning DevSecOps pipelines with PCI-DSS requirements

Module 7: Security Monitoring & Incident Response

- Continuous security monitoring strategies
- Logging, alerting, and dashboard implementations
- Threat detection and anomaly analysis
- Incident response planning and workflow
- Post-incident analysis and remediation
- Case Study: Detecting and responding to a live cyberattack

Module 8: Advanced DevSecOps Practices

- Automating security across the software supply chain
- Integrating third-party dependency scanning
- Using AI and machine learning for threat detection
- Metrics and KPIs for continuous improvement
- Organizational culture and adoption strategies
- Case Study: Scaling DevSecOps across multiple teams in an enterprise

Training Methodology

- Instructor-led presentations and conceptual briefings
- Hands-on lab exercises with CI/CD and security tools
- Case study analysis for real-world DevSecOps scenarios
- Group activities and collaborative problem-solving sessions
- Practical templates and checklists for pipeline security and compliance
- Continuous assessment, feedback sessions, and action planning

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
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 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