EC-Council Certified DevSecOps Engineer (ECDE)

ID ECDE **Price** CHF 3,300.—(excl. VAT) **Duration** 3 days

Who should attend

- C|ASE-certified professionals
- Application security professionals
- DevOps engineers
- Software engineers and testers
- IT security professionals
- Cybersecurity engineers and analysts
- Anyone with prior knowledge of application security who wants to build their career in DevSecOps

Prerequisites

Students should have an understanding of application security concepts.

Course Objectives

- Understand DevOps security bottlenecks and discover how the culture, philosophy, practices, and tools of DevSecOps can enhance collaboration and communication across development and operations teams.
- Understand the DevSecOps toolchain and how to include security controls in automated DevOps pipelines.
- Integrate Eclipse and GitHub with Jenkins to build applications.
- Align security practices like security requirement gathering, threat modeling, and secure code reviews with development workflows.
- Integrate threat modeling tools like Threat Dragon, ThreatModeler, and Threatspec; manage security requirements with Jira and Confluence; and use Jenkins to create a secure CI/CD pipeline.
- Understand and implement continuous security testing with static, dynamic, and interactive application security testing and SCA tools (e.g., Snyk, SonarQube, StackHawk, Checkmarx SAST, Debricked, WhiteSource Bolt).
- Integrate runtime application selfprotection tools like Hdiv, Sqreen, and Dynatrace that protect applications during runtime with fewer false positives and remediate known vulnerabilities.
- Integrate SonarLint with the Eclipse and Visual Studio Code IDEs.
- Implement tools like the JFrog IDE plugin and the Codacy platform.
- Integrate automated security testing into a CI/CD pipeline using Amazon CloudWatch; Amazon Elastic Container Registry; and AWS CodeCommit, CodeBuild, CodePipeline, Lambda, and Security Hub.
- Implement various automation tools and practices, including Jenkins, Bamboo, TeamCity, and Gradle.
- Perform continuous vulnerability scans on data and product builds using automated tools like Nessus, SonarCloud, Amazon Macie, and Probely.
- Implement penetration testing tools like gitGraber and GitMiner to secure CI/CD pipelines.
- Use AWS and Azure tools to secure applications.
- Integrate automated tools to identify security misconfigurations that could expose sensitive information and result in attacks.
- Understand the concept of infrastructure as code and provision and configure infrastructure using tools like Ansible, Puppet, and Chef.
- Audit code pushes, pipelines, and compliance using logging and monitoring tools like Sumo Logic, Datadog, Splunk, the ELK stack, and Nagios.
- Use automated monitoring and alerting tools (e.g., Splunk, Azure Monitor, Nagios) and create a real-time alert and control system.
- Integrate compliance-as-code tools like Cloud Custodian and the DevSec framework to ensure that organizational regulatory or compliance requirements are met without hindering production.
- Scan and secure infrastructure using container and image scanners (Trivy and Qualys) and infrastructure security scanners (Bridgecrew and Checkov).
- Integrate tools and practices to build continuous feedback into the DevSecOps pipeline using Jenkins and Microsoft Teams email notifications.
- Integrate alerting tools like Opsgenie with log management and monitoring tools to enhance operations performance and security.

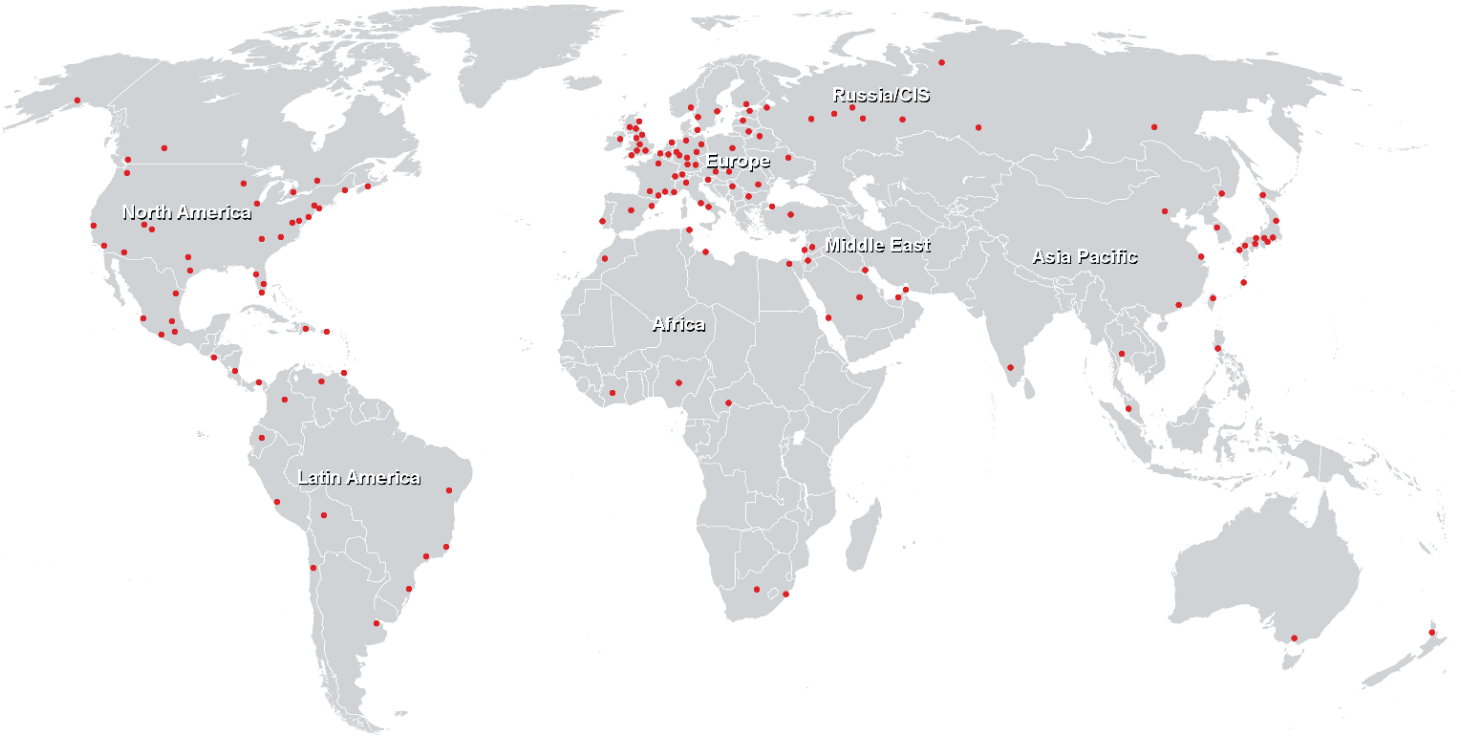
Course Content

- Understanding DevOps Culture
- Introduction to DevSecOps
- DevSecOps Pipeline—Plan Stage
- DevSecOps Pipeline—Code Stage
- DevSecOps Pipeline—Build and Test Stage

- DevSecOps Pipeline—Release and Deploy Stage
- DevSecOps Pipeline—Operate and Monitor Stage

EC-Council Certified DevSecOps Engineer (ECDE)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch