Iverson Associates Sdn Bhd (303330-M)
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my

Module Title : E|CDE: Certified DevSecOps Engineer
Duration : 3 days

Overview

EC-Council Certified DevSecOps Engineer (E|CDE) is a hands-on, instructor-led comprehensive DevSecOps certification program that helps professionals build the essential skills to design, develop, and maintain secure applications and infrastructure.

- The E|CDE covers both on-premises and cloud-native environments (including AWS Cloud and Microsoft Azure) with 80+ labs from the creators of the world's number one ethical hacking program, the Certified Ethical Hacker (C|EH).
- Designed and developed by SMEs with contributions by experienced DevSecOps professionals from around the world.

Why E|CDE?

- Adding security to a DevOps skill set enhances career prospects.
- The information provided in the E|CDE course is complemented with labs to help learners hone their practical skills and become industry ready.
- This course teaches students how to use various DevSecOps tools and create secure code throughout the software development life cycle.
- Participants gain familiarity with DevSecOps tools that enable the secure development of software and web applications, both on premises and in the cloud.
- The E|CDE course focuses on application DevSecOps and also provides insights into infrastructure DevSecOps.
- The integration of today's most popular and important tools is illustrated at each stage of the DevOps life cycle.
- The E|CDE program helps DevSecOps engineers develop and enhance their knowledge and skills in securing applications at all stages of the DevOps pipeline.

Target Audience

- C|ASE-certified professionals
- Application security professionals
- DevOps engineers
- IT security professionals
- Cybersecurity engineers and analysts

- Software engineers and testers
- Anyone with prior knowledge of application security who wants to build a career in DevSecOps

Prerequisites

Students should have an understanding of application security concepts.

What will students learn?

- 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 Outline

Module 1: Understanding DevOps Culture
Module 2: Introduction to DevSecOps
Module 3: DevSecOps Pipeline—Plan Stage
Module 4: DevSecOps Pipeline—Code Stage
Module 5: DevSecOps Pipeline—Build and Test Stage
Module 6: DevSecOps Pipeline—Release and Deploy Stage
Module 7: DevSecOps Pipeline—Operate and Monitor Stage

The Exam

EXAM TITLE	**: EC-Council Certified DevSecOps Engineer (E|CDE)**
EXAM CODE	**: 312-97**
# OF QUESTIONS	**: 100**
DURATION	**: 4 Hours**
AVAILABILITY	**: ECC Exam Portal**
TEST FORMAT	**: Multiple choice**
PASSING SCORE	**: 70%**