EC-Council's Certified DevSecOps Engineer (EICDE)

Duration : 5 Hari

DevSecOps Engineer Certification Overview

EC-Council's Certified DevSecOps Engineer (EICDE) 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 ECDE is a perfect blend of theoretical and practical knowledge of DevSecOps in your on-premises and cloud-native (AWS and Azure) environment.
- The program focuses on the application DevSecOps and provides insights into infrastructure DevSecOps.
- It helps DevSecOps Engineers develop and enhance their knowledge and skills in securing applications in all DevOps stages.

What Will You 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.
- Integrate Eclipse and GitHub with Jenkins to build applications.
- 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.
- Integrate runtime application self-protection tools like Hdiv, Sqreen, and Dynatrace to protect applications during runtime with fewer false positives and remediate known vulnerabilities.
- Implement tools like the Jfrog IDE plugin and the Codacy platform.
- Implement various automation tools and practices, including Jenkins, Bamboo, TeamCity, and Gradle.
- Implement penetration testing tools like gitGraber and GitMiner to secure CI/CD pipelines.

- Integrate automated tools to identify security misconfigurations that could expose sensitive information and result in attacks.
- Audit code pushes, pipelines, and compliance using logging and monitoring tools like Sumo Logic, Datadog, Splunk, the ELK stack, and Nagios.
- 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.
- Integrate tools and practices to build continuous feedback into the DevSecOps pipeline using Jenkins and Microsoft Teams email notifications.
- Understand the DevSecOps toolchain and how to include security controls in automated DevOps pipelines.
- Align security practices like security requirement gathering, threat modeling, and secure code reviews with development workflows.
- 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 SonarLint with the Eclipse and Visual Studio Code IDEs.
- Integrate automated security testing into a CI/CD pipeline using Amazon CloudWatch, Amazon Elastic Container Registry, AWS CodeCommit, CodeBuild, CodePipeline, Lambda, and Security Hub.
- Continuously scan data and product builds for vulnerabilities using automated tools like Nessus, SonarCloud, Amazon Macie, and Probely.
- Use AWS and Azure tools to secure applications.
- Understand the concept of infrastructure as code and provision and configure infrastructure using tools like Ansible, Puppet, and Chef.
- Automate monitoring and alerting tools (e.g., Splunk, Azure Monitor, Nagios) to create a real-time alert and control system.
- Scan and secure infrastructure using container and image scanners (Trivy and Qualys) and infrastructure security scanners (Bridgecrew and Checkov).
- Integrate alerting tools like Opsgenie with log management and monitoring tools to enhance operations performance and security.

Why Choose DevSecOps Engineer

The shift in company culture and employee mindset to prioritize data security considerations has increased the adoption of DevSecOps. Organizations have Identified that Application developers, DevOps professionals, and software engineers experience burnout due to security checks that take place at the end stage of deployment. These checks make the developer revisit the entire lifecycle loop, reducing productivity and increasing the likelihood of errors. This only worsens the problem, leading to a talent drought in the industry.

At its core, DevSecOps presents a transformative approach to software development by integrating security into every phase of the process. The DevSecOps certification is a gateway to

enhanced skills, enabling professionals to create secure and efficient software systems. This methodology ensures that security isn't an afterthought but an Integral part of development, catering to the evolving landscape's demands for robust and safe applications. Adopting DevSecOps means embracing an approach that prioritizes security from the outset, fostering resilience in an increasingly security-focused industry.

Who Is It For?

- CASE-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

Course Outline

- Module 01: Understanding DevOps Culture
- Module 02: Introduction to DevSecOps
- Module 03: DevSecOps Pipeline-Plan Stage

- Module 04: DevSecOps Pipeline-Code Stage
- Module 05: DevSecOps Pipeline-Build and Test Stage
- Module 06: DevSecOps Pipeline-Release and Deploy Stage
- Module 07: DevSecOps Pipeline-Operate and Monitor Stage