EC-Council Certified DevSecOps Engineer (E|CDE)

EC-Council – Certified DevSecOps Engineer (E|CDE)

The World’s No. 1 Ethical Hacking Certification for 20 Years

За Курса:

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.

The E|CDE 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 application DevSecOps and provides insights into infrastructure DevSecOps.

It helps DevSecOps Engineers develop and enhance their knowledge and skills in securing the application in all the stages of DevOps.

Цели – Какво ще научите:

What You Will 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 that 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, threatmodeling, 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; and AWS CodeCommit, CodeBuild, CodePipeline, Lambda, and Security Hub.
- Perform continuous vulnerability scans on data and product builds 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.
- Use automated monitoring and alerting tools (e.g., Splunk, Azure Monitor, Nagios) and 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

---

Формат на курса:

[table id=1 /]

Език на курса:

[table id=2 /]

Учебни Материали:

Учебните материали са достъпни в електронен формат. Могат да се ползват online/offline на всяко устройство. Неограничен достъп.

Лабораторна среда:

След завършване получавате:

[table id=3 /]

Продължителност:

- 3 working days (09:00 – 17:00 / 9:00 am – 5:00 pm) UTC +2 (contact us for another Time Zone)

or

- **24 learning hours after hours (2 weeks, classes are held 2 times a week in one of the following options):**
- Sat. and Sun. 10:00 – 14:00 or 14:00 – 18:00 or 18:00 – 22:00
- Mon. and Wed. 19:00 – 23:00

- Tue. or Thu. 19:00 – 23:00

Плащане:

Предстоящи Курсове:

[tribe_events_list category=”ceh”]

За повече информация използвайте формата за контакт.

Ще се свържем с Вас за потвърждаване на датите.

All EC-Council Course Schedules

[tribe_events_list category=”ec-council”]

CEHv12 Brochure.cleaned