EC-Council Certified DevSecOps Engineer (ECDE)

Category: Networking & Security | **Vendor:** EC-Council

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified DevSecOps Engineer EC-Council’s Certified DevSecOps Engineer (E|CDE) v2 is a lab-intensive

Course Overview

EC-Council’s Certified DevSecOps Engineer (E|CDE) v2 is a lab-intensive, practical course that incorporates the use of AI in DevSecOps and equips professionals with relevant skills to design, develop, and maintain secure applications and infrastructure. It covers both application and infrastructure in on-premises and the top 3 cloud-native platforms—AWS, Azure, and GCP.

About This Course

EC-Council’s Certified DevSecOps Engineer (E|CDE) v2 is a lab-intensive, practical course that incorporates the use of AI in DevSecOps and equips professionals with relevant skills to design, develop, and maintain secure applications and infrastructure. It covers both application and infrastructure in on-premises and the top 3 cloud-native platforms—AWS, Azure, and GCP.

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 & Entry Requirements

General Prerequisites:

Students should have an understanding of application security concepts.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Learn to integrate Eclipse and GitHub with Jenkins to streamline application development and build processes
- Learn to integrate threat modeling tools like Threat Dragon, ThreatModeler, and Threatspec
- Integrate Jira and Confluence to effectively manage security requirements throughout the development lifecycle
- Learn to integrate security plugins, scanners, and software composition analysis (SCA) tools within IDEs to detect and mitigate vulnerabilities early in development, following a Shift-Left security approach
- Use Jenkins to create and manage secure CI/CD pipelines
- Gain expertise in using various SAST (Snyk, SonarQube, and Checkmarx), DAST (Stackhawk, OWASP ZAP, and Invicti), IAST (CxFlow IAST and Invicti Shark), and SCA (Debricked, Mend, and OWASP Dependency-Check) tools for comprehensive security testing
- Integrate RASP tools like Contrast Security, Datadog, and Dynatrace to protect applications during runtime with minimal false positives and effective vulnerability remediation
- Learn to integrate tools like SonarLint with Eclipse, Visual Studio, and VS Code to enhance code quality and security within the development environment
- Implement tools such as JFrog Security IDE Plugin, Snyk ID, and Codacy to automate security testing within the CI/CD pipeline
- Conduct continuous vulnerability scans on product builds using automated scanning tools like Nessus, SonarQube, SonarCloud, Amazon Macie, and Probely Vulnerability Scanning
- Use penetration testing tools like GitGraber, Gitleaks, and GitMiner to secure the CI/CD pipeline against vulnerabilities
- Provision and configure infrastructure using infrastructure as code (IaC) tools like Ansible, Puppet, and Chef
- Implement comprehensive logging and monitoring using tools like Sumo Logic, Datadog, Splunk, ELK, and Nagios to audit everything from code pushes to compliance activities
- Use automated monitoring and alerting tools such as Splunk, Paessler PRTG, and Nagios to build real-time alerting and control systems
- Integrate Compliance as Code (CaC) tools like Cloud Custodian and DevSec to meet regulatory requirements without disrupting production
- Learn to scan and secure infrastructure using container and image scanners (Trivy, Qualys) and infrastructure security scanners (Prisma Cloud, Checkov)

- Integrate continuous feedback mechanisms into the DevSecOps pipeline using tools like email notifications in Jenkins and Microsoft Teams
- Integrate alerting tools like OpsGenie with log management and monitoring tools to improve operational performance and security
- Integrate tools like Incident.io, PagerDuty, and Splunk for effective incident response within the DevSecOps pipeline

Detailed 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

Skills You Will Learn:

- Learn to integrate Eclipse and GitHub with Jenkins to streamline application development and build processes
- Learn to integrate threat modeling tools like Threat Dragon, ThreatModeler, and Threatspec
- Integrate Jira and Confluence to effectively manage security requirements throughout the development lifecycle
- Learn to integrate security plugins, scanners, and software composition analysis (SCA) tools within IDEs to detect and mitigate vulnerabilities early in development, following a Shift-Left security approach
- Use Jenkins to create and manage secure CI/CD pipelines
- Gain expertise in using various SAST (Snyk, SonarQube, and Checkmarx), DAST (Stackhawk, OWASP ZAP, and Invicti), IAST (CxFlow IAST and Invicti Shark), and SCA (Debricked, Mend, and OWASP Dependency-Check) tools for comprehensive security testing
- Integrate RASP tools like Contrast Security, Datadog, and Dynatrace to protect applications during runtime with minimal false positives and effective vulnerability remediation
- Learn to integrate tools like SonarLint with Eclipse, Visual Studio, and VS Code to enhance code quality and security within the development environment
- Implement tools such as JFrog Security IDE Plugin, Snyk ID, and Codacy to automate security testing within the CI/CD pipeline
- Conduct continuous vulnerability scans on product builds using automated scanning tools like Nessus, SonarQube, SonarCloud, Amazon Macie, and Probely Vulnerability Scanning
- Use penetration testing tools like GitGraber, Gitleaks, and GitMiner to secure the CI/CD pipeline against vulnerabilities
- Provision and configure infrastructure using infrastructure as code (IaC) tools like Ansible, Puppet, and Chef
- Implement comprehensive logging and monitoring using tools like Sumo Logic, Datadog, Splunk, ELK, and Nagios to audit everything from code pushes to compliance activities
- Use automated monitoring and alerting tools such as Splunk, Paessler PRTG, and Nagios to build real-time alerting and control systems
- Integrate Compliance as Code (CaC) tools like Cloud Custodian and DevSec to meet regulatory requirements without disrupting production
- Learn to scan and secure infrastructure using container and image scanners (Trivy, Qualys) and infrastructure security scanners (Prisma Cloud, Checkov)
- Integrate continuous feedback mechanisms into the DevSecOps pipeline using tools like email notifications in Jenkins and Microsoft Teams
- Integrate alerting tools like OpsGenie with log management and monitoring tools to improve operational performance and security
- Integrate tools like Incident.io, PagerDuty, and Splunk for effective incident response within the DevSecOps pipeline

Frequently Asked Questions

Q: What delivery options are available for EC-Council Certified DevSecOps Engineer (ECDE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The EC-Council Certified DevSecOps Engineer (ECDE) course helps prepare you for the Certified DevSecOps Engineer EC-Council’s Certified DevSecOps Engineer (E|CDE) v2 is a lab-intensive certification path.

Q: How many CPD hours does this course provide?

The 3-day EC-Council Certified DevSecOps Engineer (ECDE) course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council Certified DevSecOps Engineer (ECDE) training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council Certified DevSecOps Engineer (ECDE)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council Certified DevSecOps Engineer (ECDE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: EC-Council Certified DevSecOps Engineer, Specialist, ECDE

Q: Why choose Nexus Human for EC-Council Certified DevSecOps Engineer (ECDE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council Certified DevSecOps Engineer (ECDE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)