EC-Council

E|CDE

EC-Council | Certified DevSecOps Engineer

EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER

Master AI-Enhanced DevSecOps to Secure Modern Development Pipelines

E|CDE

EC-Council | Certified DevSecOps Engineer

According to Verified Market Research, the DevSecOps market was valued at USD 8.15 billion in 2024 and is projected to reach USD 58.32 Billion by 2031, ascending at a CAGR of 30.76% from 2024 to 2031. [1].

The growth of the DevSecOps market is fueled by a surge in sophisticated cyberattacks, increasing the need for quick delivery of secure applications. Organizations are looking for certified DevSecOps engineers, with competitive salaries for freshers as well as experienced professionals, to help them with developing quick and secure software products. However, due to a lack of skilled DevSecOps professionals, most of the organizations are unable to find suitable candidates and the position remains vacant for years.

Link 1 - https://www.verifiedmarketresearch.com/product/devsecops-market/

EC-Council Certified DevSecOps Engineer (E|CDE) v2: AI-Powered Tools and Cloud Expertise

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.

Key Enhancements in E|CDE v2

- Updated content to align with the latest advancements in technologies and processes within DevSecOps
- Incorporates Google Cloud Platform DevSecOps tools and practices
- Includes incident response and Business Continuity and Disaster Recovery (BCDR) practices
- Incorporates the use of AI, including AI-powered tools for DevOps/DevSecOps pipeline, secure code review, and Static Application Security Testing (SAST)
- 70% lab-intensive with over 100 labs, making it a more hands-on and practical course
- Covers security across all 8 DevOps lifecycle stages—plan, code, build, test, deploy, release, operate, and monitor

Why Choose E|CDE v2

- You will be well-prepared to manage security incidents and maintain operational resilience
- You will discover how to leverage AI-powered tools for the DevSecOps pipeline, thereby enhancing automation
- You will gain familiarity with various open-source and commercial third-party DevSecOps tools, which enable the secure development of software and web applications within an organization's internal IT infrastructure as well as in a public cloud environment
- You will gather insights into application DevSecOps as well as infrastructure DevSecOps
- You will hone your skills to detect and remediate security issues while developing application codes by utilizing automated application security testing such as SAST, DAST, IAST, and RASP

How E|CDE v2 Can Secure Cloud Environments

- Cloud security usually happens outside the software development lifecycle. However, EC-Council's E|CDE program enables teams to address cloud security issues via CI/CD pipelines and fix issues directly at the source.

How E|CDE v2 Can Secure AWS Cloud

- AWS offers a set of tools and services to identify vulnerabilities at different stages of the development life cycle
- The E|CDE v2 program covers how to integrate all the necessary AWS tools to identify security vulnerabilities at various stages of the DevSecOps pipeline

How E|CDE v2 Can Secure Microsoft Azure

- With the rising sophistication of cyberattacks, Azure DevSecOps combines GitHub and Azure products and services to help DevOps and SecOps teams collaborate in building more secure apps. The E|CDE v2 program covers all the latest tools and integrations in the Azure DevSecOps module

How E|CDE v2 Can Secure GCP

- GCP Secret Manager is utilized to securely manage sensitive data, while tools like Synk for SCA and Intruder for DAST strengthen application securitys
- Vulnerability scanning is achieved through Nessus integration and the Cloud Security command Center provides comprehensive monitoring of GCP resources to detect and mitigate threats
- Google cloud Armor is employed as a robust web application firewall to protect applications and automated patch management is enabled through GCP VM Manager to ensure continuous system updates

Gain a Competitive Advantage with the E|CDE v2

- It is the most comprehensive DevSecOps certification program, which focuses on integrating security in the plan, code, build, test, deploy, release, operate, and monitor stages of the DevOps lifecycle
- It is the most lab-intensive DevSecOps certification program, which covers 100+ guided, hands-on labs delivered in the form of virtual online labs and offline classroom labs. E|CDE covers 35 on-premises-focused labs, 28 AWS-focused labs, 28 Azure-focused labs, and 15 GCP-focused labs in E|CDE
- It is the most sought-after DevSecOps certification program, covering an enhanced and broad range of DevSecOps tools and practices widely used across industries

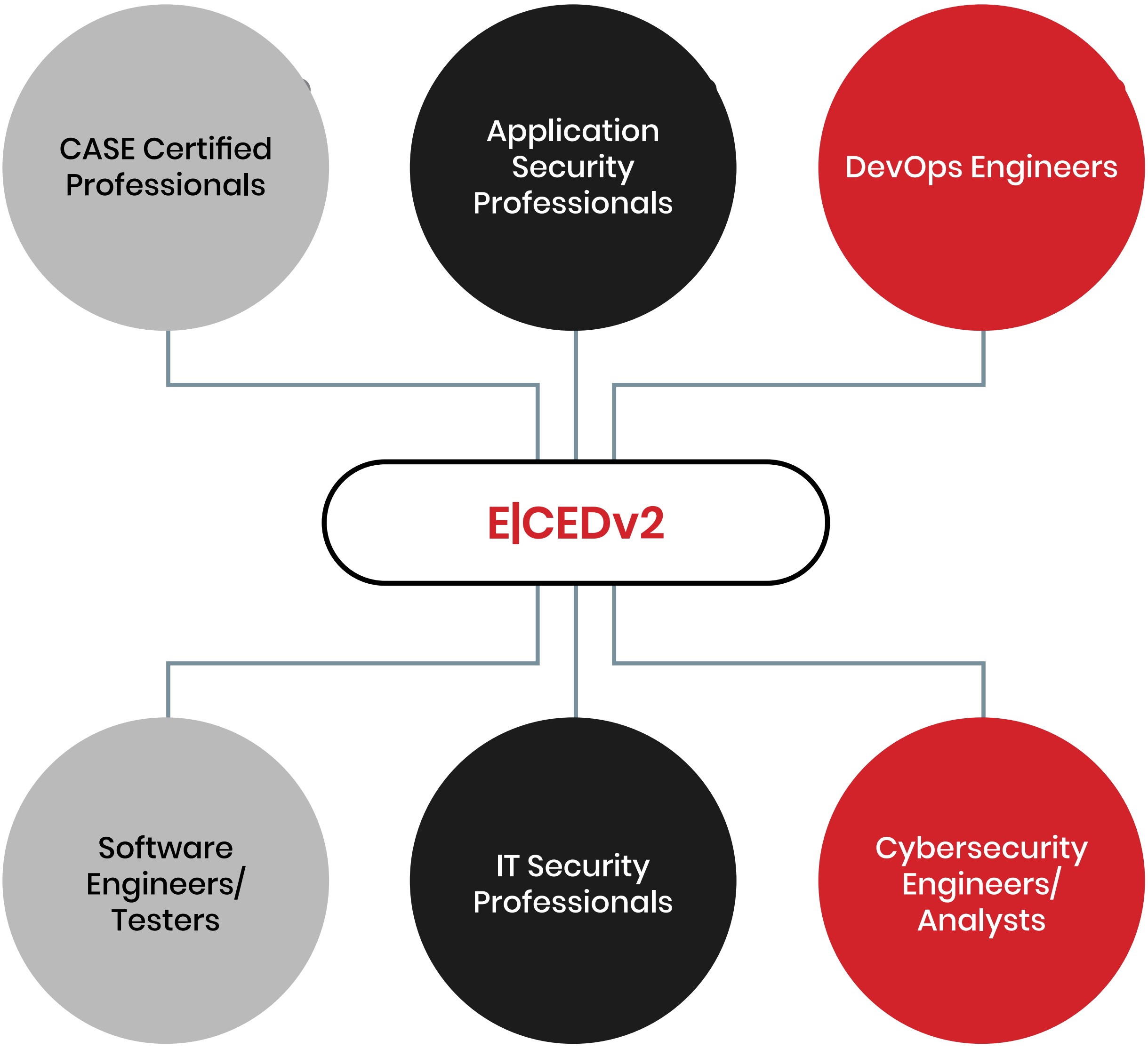
What You'll Learn

- 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

Who Can Benefit From the E|CDE v2?

Anyone with prior knowledge of application security, who wants to build a career in DevSecOps.

The intended professionals for the course are:


CASE Certified Professionals
Application Security Professionals
DevOps Engineers
E|CEDv2
Software Engineers/ Testers
IT Security Professionals
Cybersecurity Engineers/ Analysts

Job Roles Aligned to E|CDE v2 Certification

- DevSecOps Engineer/Senior DevSecOps Engineer
- Cloud DevSecOps Engineer
- Azure DevSecOps Engineer
- AWS DevSecOps Engineer
- DevSecOps Analyst
- DevSecOps Specialist
- DevSecOps Systems Administrator
- DevSecOps System Engineer
- DevSecOps Consultant
- DevSecOps CI/CD Engineer
- Infrastructure DevSecOps Engineer

E|CDE Training Information

Title of the Course: **EC-Council Certified DevSecOps Engineer (E|CDE) v2**

Training: **3 Days**

Training Timing: **9:00 AM to 5:00 PM**

Training Options:

- **Instructor-led Training (ILT):**
  Available globally through EC-Council's Authorized Training Partners. This mode offers you the benefit of learning from experienced, certified EC-Council instructors along with your peers.
- **iWeek (Synchronous Online Learning):**
  Synchronous online learning led by an instructor, allowing students to attend the ECDE course from anywhere.
- **iLearn (Asynchronous Online Learning):**
  An asynchronous, self-study environment that delivers the ECDE course in a streaming video format.

Module	Learning Objectives
Module 01 Understanding DevOps Culture	This module introduces the principles and concepts of DevOps. It covers the cultural and technical foundations of DevOps, emphasizing collaboration between development and operations teams. Key topics include the significance of automation, continuous integration/deployment (CI/CD), and fostering a culture of continuous improvement. The module also covers DevOps values, benefits, and challenges, along with the role of collaboration, communication, and feedback loops in achieving faster and more reliable software delivery.
Module 02 Introduction to DevSecOps	This module covers the foundational concepts of DevSecOps, focusing on integrating security into the DevOps lifecycle. It explains the principles and importance of DevSecOps, emphasizing the shift from traditional security approaches to a more collaborative, automated, and continuously integrated security approach. The module introduces key components such as culture, automation, monitoring, and feedback loops, along with commonly used tools and practices. It also discusses the benefits of adopting DevSecOps, addresses its key challenges, and provides insights into establishing a DevSecOps culture within organizations.
Module 03 DevSecOps Pipeline – Plan Stage	This module covers the planning phase of the DevSecOps pipeline. It focuses on identifying security requirements, conducting threat modeling, and establishing a security-focused plan. It also highlights the importance of collaboration between development, security, and operations teams to ensure alignment with security goals.
Module 04 DevSecOps Pipeline – Code Stage	This module discusses secure coding practices and the integration of security into the development process. Topics include static code analysis, secure coding guidelines, and the implementation of security controls within the integrated development environment (IDE). Developers learn to write secure code using industry best practices.
Module 05 DevSecOps Pipeline – Build and Test Stage	In this module, learners explore how to integrate security into the build and testing processes. It covers automated security testing, including SAST and DAST. It also emphasizes the use of continuous integration (CI) pipelines.
Module 06 DevSecOps Pipeline – Release and Deploy Stage	This module explains how to maintain security during the release and deployment phases. It highlights secure deployment techniques, IaC security, and the use of container security tools. It also covers release management and secure configuration practices.
Module 07 DevSecOps Pipeline – Operate and Monitor Stage	The final module focuses on securing the operational environment and monitoring applications for security incidents. It includes topics like logging, monitoring, and incident detection and response. It also discusses continuous security monitoring using security information and event management (SIEM) tools.

E|CDE Exam Information

- Exam Number: **312-97**
- Questions: **100**
- Passing Score: **70%**
- Duration: **4 hours**
- Test format: **Multiple-Choice**
- Passing score: **70%**

Course Prerequisites

Students should have an understanding of application security concepts.

Stay Ahead in Cybersecurity

In an era where cybersecurity is paramount, the E|CDE v2 equips you with the knowledge and skills to proactively embed security into every phase of development. By mastering these competencies, you enhance your ability to safeguard applications and infrastructure, making you an invaluable asset in the cybersecurity landscape.

For more information and enrollment details, please visit EC-Council's official website.

Note: The E|CDE v2 program is continually updated to reflect the latest advancements in DevSecOps practices and technologies.

EC-Council Recognition, Endorsement, and Mapping

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

ANAB
ANSI National Accreditation Board

CYBER WORKFORCE QUALIFICATION PROGRAM
DoD 8140

nicf
NATIONAL INFOCOMM COMPETENCY FRAMEWORK
Jointly developed by IDA and WDA

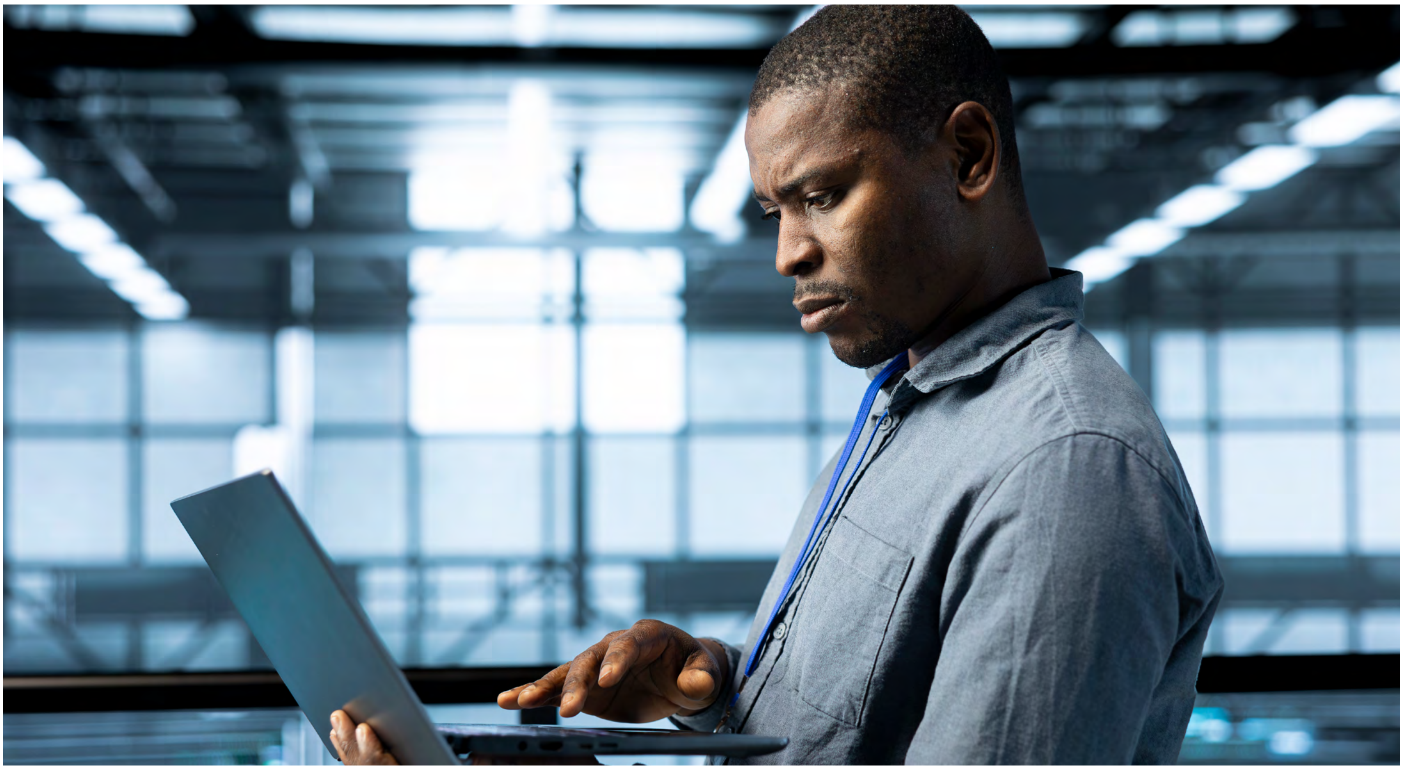
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

MSC
MALAYSIA
Spearheading Transformation

ANGKATAN TENTERA MALAYSIA

About EC-Council

EC-Council's sole purpose is to build and redefine the cybersecurity profession globally.



We help individuals, organizations, educators, and governments address global workforce problems through the development and curation of world-class cybersecurity education programs and their corresponding certifications and provide cybersecurity services to some of the largest businesses globally.

Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the U.S. Department of Defense, the intelligence community, NATO, and over 2000 of the best universities, colleges, and training companies, our programs have certified people in 150 countries and set the bar in the field of cybersecurity education.

Best known for the Certified Ethical Hacker program, we are dedicated to equipping over 380,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against cyber adversaries. EC-Council builds individual and organization-wide cyber capabilities through our other programs as well, including Certified Secure Computer User (CSCU), Computer Hacking Forensic Investigator (CHFI), Certified Security Analyst, Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Threat Intelligence Analyst (CTIA), Certified Incident Handler (ECIH), and the Certified Chief Information Security Officer (CCISO).

We are an ANAB ISO/IEC 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies. Founded in 2001, EC-Council employs over 400 individuals worldwide, with ten global offices in the U.S., UK, Malaysia, Singapore, India, and Indonesia. Our U.S. offices are in Albuquerque, NM, and Tampa, FL.

Learn more at eccouncil.org.

EC-Council

Building A Culture Of Security

E|CDE

EC-COUNCIL CERTIFIED DEVSECOPS ENGINEER

WE DON’T JUST TEACH DEVSECOPS SKILLS

WE TEACH APPLICATION AND INFRASTRUCTURE SECURITY FOR ON-PREMISES AND CLOUD PLATFORMS

GET LAB-INTENSIVE, HANDS-ON TRAINING NOW WITH AI TOOLS