EC-Council

E|CDE
EC-Council Certified DevSecOps Engineer

EC-Council Certified
DevSecOps Engineer

SPEED UP
DEVELOPMENT & DEPLOYMENT OF APPLICATIONS

Be on the Right Side. Shift Left.

Master Securing Applications with
80+ Skill-Based Labs Cloud-Native DevSecOps.

INDUSTRY STATISTICS

The growth of the DevSecOps market is fueled by a growing surge in cyberattacks, increasing the need for the quick delivery of secure applications.

According to IBM's Cost of a Data Breach Report 2021, the average cost of breaches between 50 million and 65 million records was USD 401 million. [1]

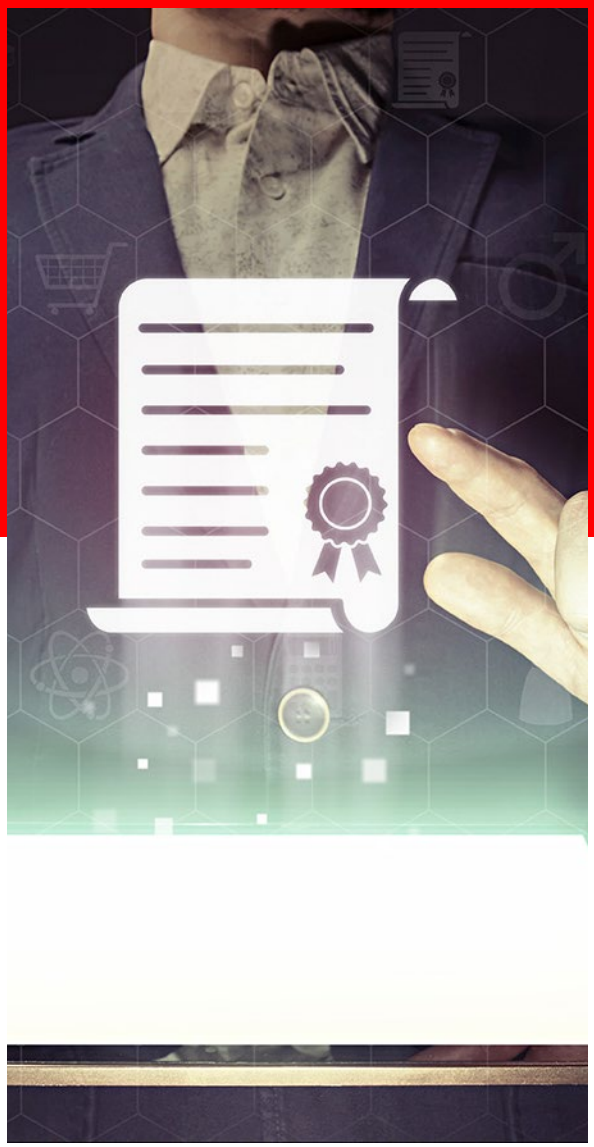
According to Identity Theft Resource Center's (ITRC) First Quarter 2022 Data Breach Analysis, there have been 398 incidents of data breaches with 13,676,543 victims. [2]

According to Verified Market Research, the DevSecOps market size was USD 3.73 billion in 2021 and is estimated to reach USD 41.66 billion by 2030, growing at a CAGR of 30.76% from 2022 to 2030. [3]

[1]: https://www.ibm.com/downloads/cas/OJDVQGRY
[2]: https://www.idtheftcenter.org/wp-content/uploads/2022/04/20220413_One-Pager_Q1-2022-Data-Breach-Analysis.pdf
[3]: https://www.verifiedmarketresearch.com/product/devsecops-market/

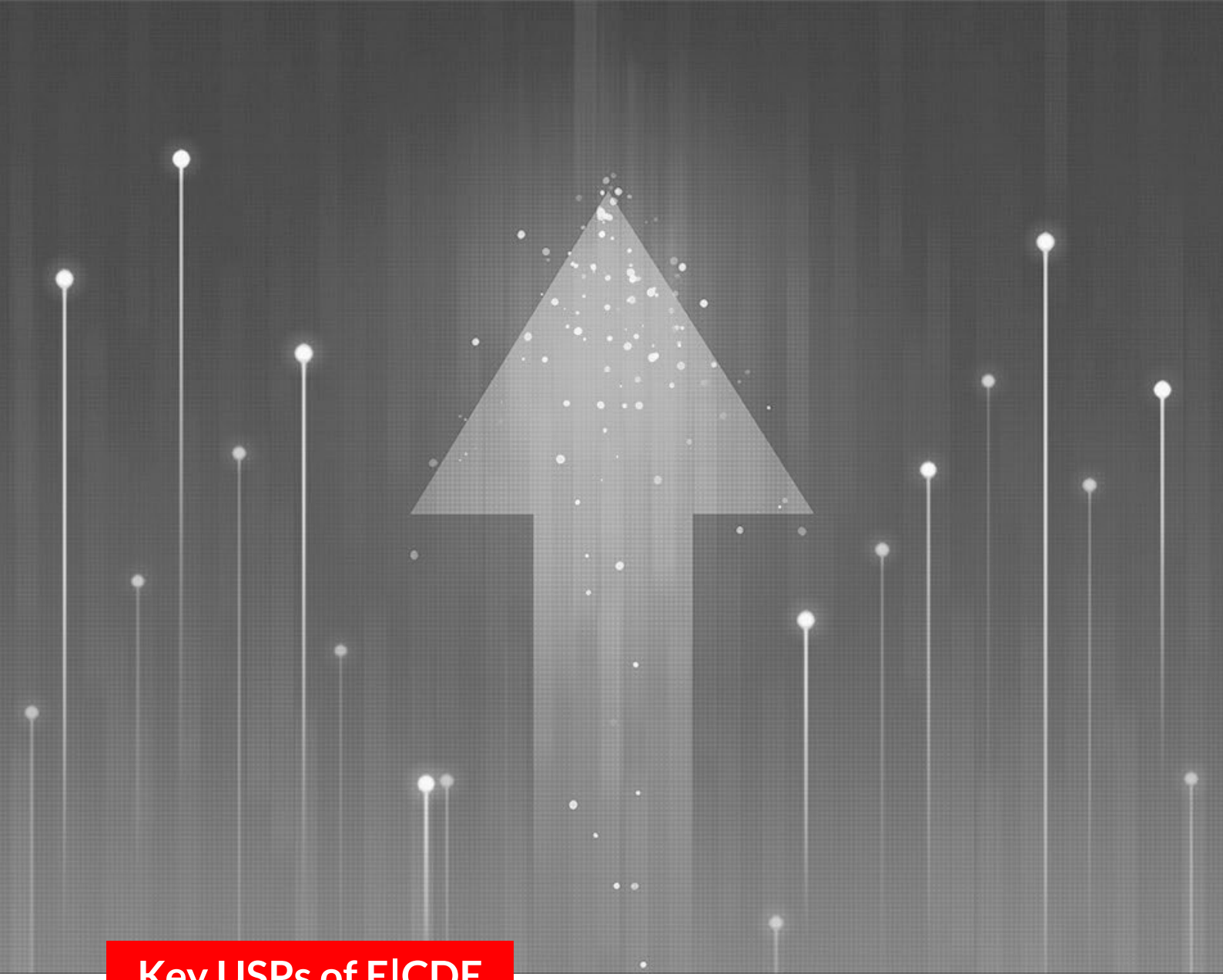
EC-Council Certified DevSecOps Engineer (E|CDE) Certification

Speed up the digital transformation of on-premises and cloud-native environments with the E|CDE certification, a lab-intensive program with 70% of the curriculum dedicated to labs and 30% to theory.



EC-Council's Certified DevSecOps Engineer (E|CDE) is a hands-on, instructor-led comprehensive DevSecOps certification program that helps professionals build the essential skills needed 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.



Key USPs of E|CDE

Lab-intensive program with more than 80+ skill-based labs

Covers both application and infrastructure DevSecOps of on-premises and cloud-native platforms

Covers security aspects and tools integration at all eight DevOps stages

Mapped with real-time job roles and the responsibilities of DevSecOps Engineers

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.

How E|CDE Can Secure Cloud Environments

Cloud security usually happens outside the software development life cycle. 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 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 program covers how to integrate all the necessary AWS tools to identify security vulnerabilities at various stages of the DevSecOps pipeline.

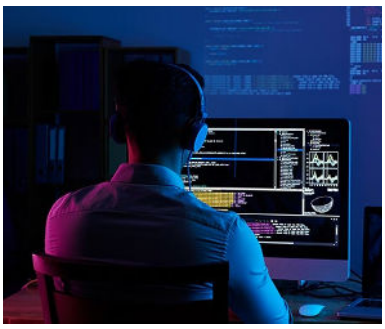
How E|CDE Can Secure Microsoft Azure

Azure DevSecOps combines GitHub and Azure products and services to help DevOps and SecOps teams collaborate in building more secure apps as new types of cyberattacks rise. The E|CDE program covers all the latest tools and integrations in the Azure DevSecOps module.

Why Should You Obtain E|CDE Certification?

DevSecOps is a logical extension of DevOps that builds security into each application. It is a defense system that ensures that developed applications and infrastructures are less vulnerable to cyberattacks.

Every application in the world needs a security checkpoint; hence, the skills of DevSecOps engineers are required.

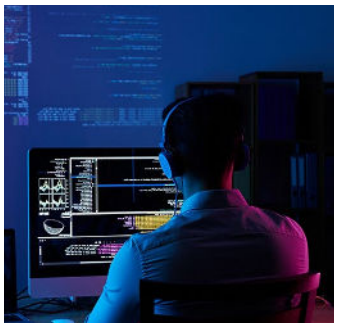


Every firm or freelancer developing and testing applications needs DevSecOps skills.

Gain a Competitive Advantage with the E|CDE

Flexera's 2022 State of the Cloud Report revealed that 89% of organizations have a multi-cloud strategy.[4] With businesses migrating to the cloud, implementing the DevSecOps approach can help ensure security and compliance.

E|CDE 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.

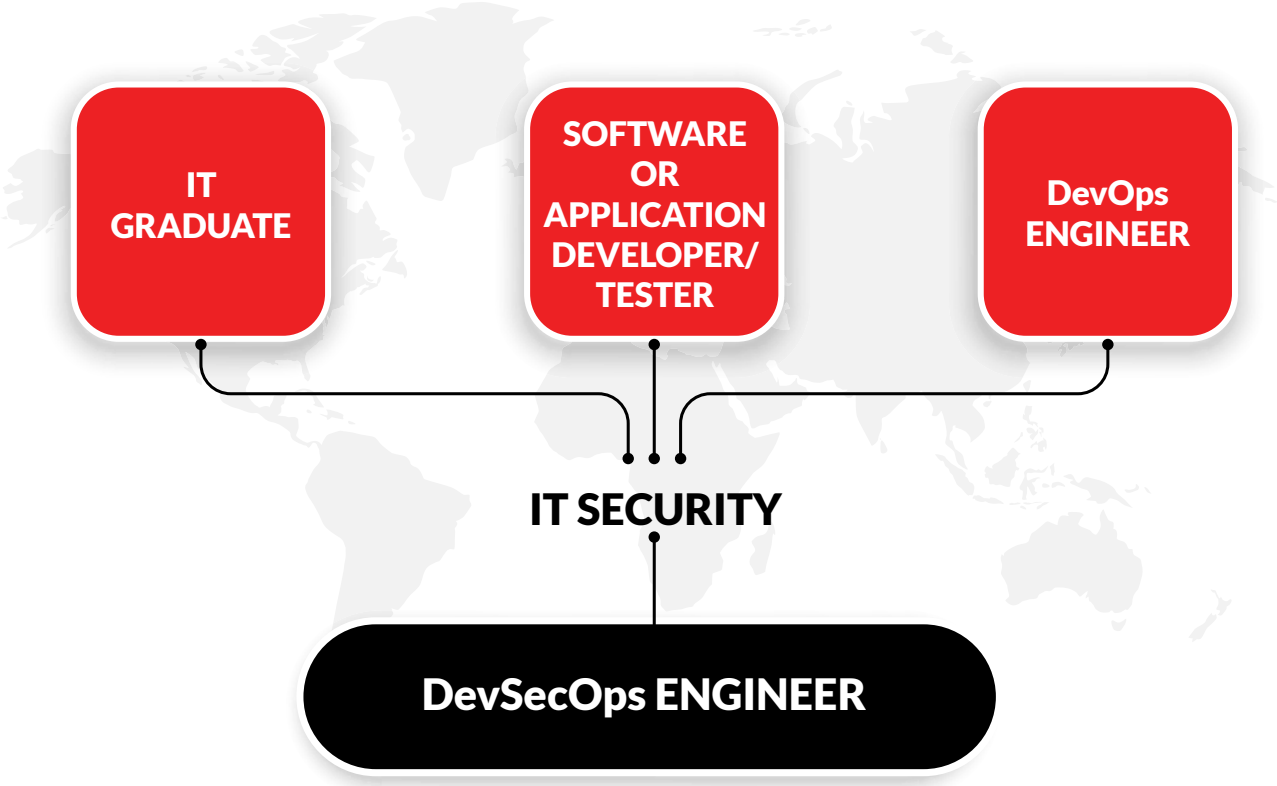


E|CDE is the most Lab intensive DevSecOps certification program which covers 80+ guided hands-on labs delivered in the form of Virtual online labs and offline Classroom labs. E|CDE covers 32 on-prem-focused labs, 32 AWS-focused labs, and 29 Azure-focused labs in E|CDE.

E|CDE is the most sought-after DevSecOps certification program, covering an enhanced and broader range of DevSecOps tools and practices widely practiced across industries.

[4]: https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2022.pdf

Career Pathways into DevSecOps Professions



Course Outline and Class information

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

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 self-protection 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.

Who Can Benefit From the E|CDE?

- 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

Job Roles Aligned with the E|CDE

- DevSecOps engineer
- Senior DevSecOps engineer
- Cloud DevSecOps engineer
- Azure DevSecOps engineer
- AWS DevSecOps engineer
- DevSecOps analyst
- DevSecOps specialist
- DevSecOps operations engineer
- DevSecOps systems administrator
- DevSecOps systems engineer
- DevSecOps consultant
- DevSecOps CI/CD engineer
- Infrastructure DevSecOps engineer

Course Prerequisites

Students should have an understanding of application security concepts.

E|CDE Training Information

Course Title: EC-Council Certified DevSecOps Engineer (E|CDE)

Training Duration: 3 Days

iLearn (Self-Study)

An asynchronous, self-study environment that delivers the E|CDE course in a streaming video format

iWeek (Live Online)

Synchronous online learning lead by an instructor, allowing students to attend the E|CDE course from anywhere

Academia

Offers the E|CDE through EC-Council Academia Partner institutions for students enrolled in applicable college or university degree programs

Training Partner Instructor-led training

The E|CDE is 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.

E|CDE Exam Information

Exam Title	Exam Code	Number of Questions
EC-Council Certified DevSecOps Engineer (E|CDE)	312-97	100

Duration	Availability	Test Format	Passing Score
4 hours	EC-Council Exam Portal	Multiple Choice	70.00%

About EC-Council

EC-Council's sole purpose is to build and refine 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 Department of Defense, Intelligence Community, NATO, and over 2000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 Countries and have set the bar in cybersecurity education.

Best known for the Certified Ethical Hacker program, we are dedicated to equipping over 230,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANSI 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and a variety of other authoritative bodies that influence the entire profession. Founded in 2001, EC-Council employs over 400 people worldwide with 10 global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at **www.eccouncil.org**

EC-Council

DevSecOps ENGINEER (E|CDE)

www.eccouncil.org