Certified Cloud Security Engineer (CCSE)

Course Overview

EC-Council's Certified Cloud Security Engineer (C|CSE) course is a specialized program curated by cloud security professionals in collaboration with subject matter experts from around the globe. C|CSE is a hands-on learning cortication course that adopts a detailed and methodological approach to teaching the fundamental concepts of cloud security. EC-Council's C|CSE program blends vendor-neutral and vendor-specific cloud security concepts, offering aspirants an unbiased learning approach. Vendor-neutral concepts emphasize universally applicable cloud security best practices, technologies, and frameworks to help individuals strengthen their grasp of the fundamentals. Vendor-specific concepts help individuals gain the practical skills needed to work with specific cloud platforms.

Benefits of CCSE:

- Offers comprehensive knowledge and practical learning of security practices, tools, and techniques used to configure widely used public cloud providers such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP).
- Enables you to learn the skills required in real-world threat scenarios from industry experts
- Plays an active role in enhancing your organization's security posture by teaching you how to plan, configure, implement, and maintain a secure cloud environment.
- Demonstrates how to perform cloud computing security audits and penetration testing to help organizations comply with the standards, policies, procedures, and regulations governing cloud environments.
- Provides a simulated environment with over 50 complex labs to equip you with skills that matter and ensure job readiness
- Is mapped with real-time job roles and responsibilities of cloud security professionals

Target Audience:

- Network Security administrators, engineers, and analysts
- Cloud administrators, engineers, and analysts

- InfoSec professionals
- Cybersecurity engineers and analyst
- CND Certified professionals
- Any other role involving network and cloud administration, management and operation

Course Outlines:

Module #	Module Topic
Module 01	**Introduction to Cloud Security**
Module 02	**Platform and Infrastructure Security in the Cloud**
Module 03	**Application Security in the Cloud**
Module 04	**Data Security in the Cloud**
Module 05	**Operation Security in the Cloud**
Module 06	**Penetration Testing in the Cloud**
Module 07	**Incident Detection and Response in the Cloud**
Module 08	**Forensics Investigation in the Cloud**
Module 09	**Business Continuity and Disaster Recovery in the Cloud**
Module 10	**Governance, Risk Management, and Compliance in the Cloud**

Module 11	Standards, Policies, and Legal Issues in the Cloud
Appendix (Self-Study)	Private, Hybrid, and Multi-Tenant Cloud Security

Exam Details:

Exam Details	CCSE (312-40)
Number of Questions	125
Test Duration	4 Hours
Test Format	Multiple Choice Questions
Test Delivery	ECC EXAM Portal
Passing Score	70%