**Iverson Associates Sdn Bhd (303330-M)**
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my



**Module Title : Certified Cloud Security Engineer (C|CSE)**
**Duration : 5 days**

## Overview

EC-Council's Certified Cloud Security Engineer (C|CSE) course is curated by cloud security professionals in association with renowned subject matter experts to deliver a mix of vendor-neutral and vendor-specific cloud security concepts. The vendor-neutral concepts focus on cloud security practices, technologies, frameworks, and principles. In contrast, the vendor-specific materials deliver the practical skills that are needed to configure specific platforms, such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). This offers candidates a well-balanced mix of theoretical and practical skills. In addition, advanced topics also cover modules on securing the cloud infrastructure by implementing regulations and standards to maintain security. EC-Council's cloud security course is mapped to the real-time job roles and responsibilities of cloud security professionals and is ideal for beginners as well as experienced cybersecurity professionals.

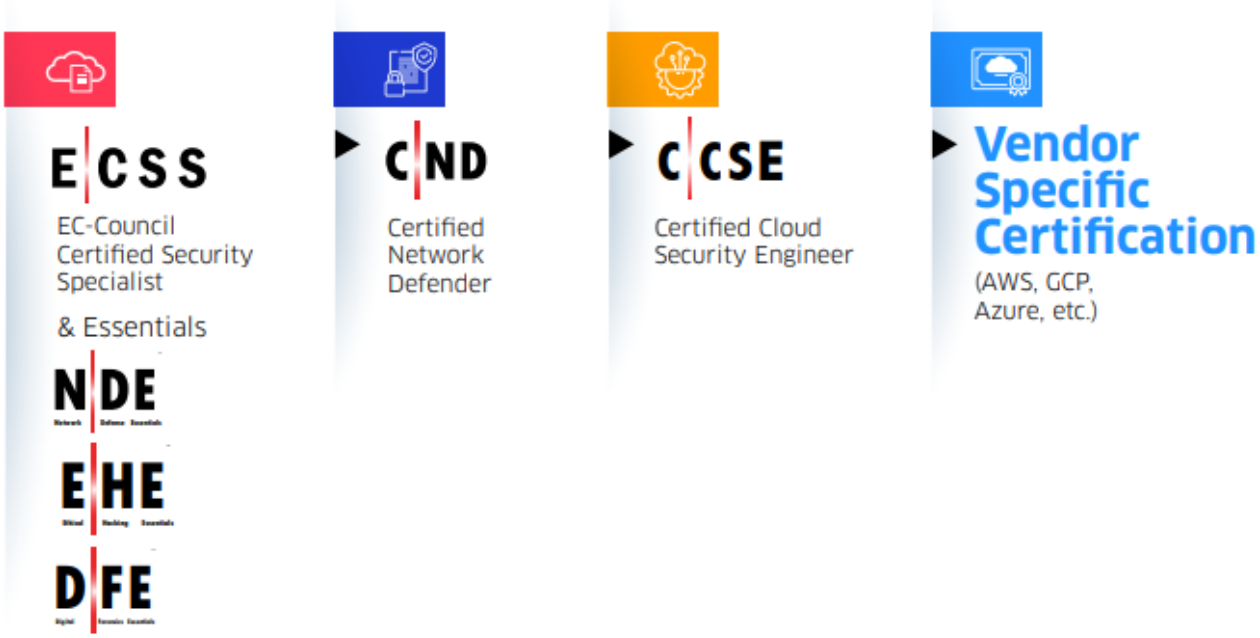
## Target Audience

- Network security engineers
- Cybersecurity analysts
- Network security analysts
- Cloud administrators and engineers
- Network security administrators
- Cloud analysts
- Cybersecurity engineers
- Those working in network and cloud management and operations

## Exam Details

- Number of Questions: 125
- Duration: 04 hours
- Availability: EC-Council Exam Portal
- Test Format: Multiple Choice

## Career Progression to Cloud Security




## Course Outline

**Module 01: Introduction to Cloud Security**

In this module, you will be presented with the core concepts of cloud computing, cloud service models, and cloud-based threats and vulnerabilities. The module highlights service provider components, such as evaluation and the shared security responsibility model, that are essential to configuring a secure cloud environment and protecting organizational resources.

**Module 02: Platform and Infrastructure Security in the Cloud**

This module explores the key components and technologies that form a cloud architecture and how to secure multi-tenant, virtualized, physical, and logical cloud components. This module demonstrates configurations and best practices for securing physical data centers and cloud infrastructures using the tools and techniques provided by Azure, AWS, and GCP.

**Module 03: Application Security in the Cloud**

The focus of this module is securing cloud applications and explaining secure software development lifecycle changes. It explains the multiple services and tools for application security in Azure, AWS, and GCP.

**Module 04: Data Security in the Cloud**

This module covers the basics of cloud data storage, its lifecycle, and various controls for protecting data at rest and data in transit in the cloud. It also addresses data storage features and the multiple services and tools used for securing data stored in Azure, AWS, and GCP.

**Module 05: Operation Security in the Cloud**

This module encompasses the security controls essential to building, implementing, operating, managing, and maintaining physical and logical infrastructures for cloud environments and the required services, features, and tools for operational security provided by AWS, Azure, and GCP.

**Module 06: Penetration Testing in the Cloud**

This module demonstrates how to implement comprehensive penetration testing to assess the security of an organization's cloud infrastructure and reviews the required services and tools used to perform penetration testing in AWS, Azure, and GCP.

**Module 07: Incident Detection and Response in the Cloud**

This module focuses on incident response (IR). It covers the IR lifecycle and the tools and techniques used to identify and respond to incidents; provides training on using SOAR technologies; and explores the IR capabilities provided by AWS, Azure, and GCP.

**Module 08: Forensics Investigation in the Cloud**

This module covers the forensic investigation process in cloud computing, including various cloud forensic challenges and data collection methods. It also explains how to investigate security incidents using AWS, Azure, and GCP tools.

**Module 09: Business Continuity and Disaster Recovery in the Cloud**

This module highlights the importance of business continuity and disaster recovery planning in IR. It covers the backup and recovery tools, services, and features provided by AWS, Azure, and GCP to monitor business continuity issues.

**Module 10: Governance, Risk Management, and Compliance in the Cloud**

This module focuses on the various governance frameworks, models, and regulations (ISO/IEC 27017, HIPAA, and PCI DSS) and the design and implementation of governance frameworks in the cloud. It also addresses cloud compliance frameworks and elaborates on the AWS, Azure, and GCP governance modules.

**Module 11: Standards, Policies, and Legal Issues in the Cloud**

This module discusses standards, policies, and legal issues associated with the cloud. It also covers the features, services, and tools needed for compliance and auditing in AWS, Azure, and GCP.

**Appendix (Self-Study): Private, Hybrid, and Multi-Tenant Cloud Security**

The appendix covers the security of private, hybrid, and multi-tenant cloud models. It lists some of the best practices for securing VMWare Cloud, AWS, GCP, Azure hybrid cloud setups, and multi-tenant clouds.

## Recommended Prerequisites

- Have working knowledge in network security management
- Basic understanding of cloud computing concepts
- You will need an account (preferably, a new free tier account) on AWS, Azure, and GCP cloud services to perform labs.