EC-Council Certified Cloud Security Engineer (CCSE) + Exam voucher

Duration: 5 Days **Course Code: ECCCSE** **Version: 2.0**

Overview:

The Certified Cloud Security Engineer (C|CSE) is a multi-cloud security certification program crafted by industry experts. It offers a holistic understanding of cloud security and empowers cybersecurity professionals to apply practical skills to build, operate, and defend their environments regardless of the selected infrastructure.
Our unique approach to designing curriculum allows C|CSE content to match the latest security tools and techniques for the AWS, Azure, and GCP platforms, as well as private and hybrid architectures. This design makes the C|CSE program a perfect blend of vendor-neutral training topics with vendor specific instruction and performance labs, offering cybersecurity professionals an unbiased learning experience.
C|CSE offers a hands-on practical approach, featuring over 85 labs to ensure candidates gain hands on experience that can be immediately applied at the workplace to anticipate and overcome cloud security challenges.
With organizations storing and processing more data than ever on multiple cloud environments, multi-cloud security is essential to organizational cyber security initiatives. According to a forecast by Markets and Markets, the multi-cloud security market is expected to grow to USD 10.5 billion by 2027, creating a significant demand across verticals such as BFSI, healthcare, telecommunications, IT, retail, ecommerce, and other industries.
Updated 12/5/2026

Target Audience:

The Certified Cloud Security Engineer (C|CSE) program is tailored for an intermediate level and is ideally suited for individuals with prior experience in cybersecurity. The program offers a comprehensive exploration of advanced cloud security concepts, equipping working professionals with a holistic perspective covering a wide range of cloud platforms and service providers. Professionals with experience in any of the below domains can apply:
- Network Security: Administrator/Engineer/Analyst:
- Cybersecurity: Engineer/Analyst
- Cloud: Administrator/Analyst/Engineer
- InfoSec professionals
- C|ND professionals
OR

Objectives:

- **After attending this cloud security course, participants will be able to gather:**
- **Generic Cloud Security Concepts**
- Fundamentals of cloud computing and its architecture
- Key concepts and components of cloud security
- Cloud deployment models (public, private, hybrid) and their associated security considerations
- Cloud service models (IaaS, PaaS, SaaS) and their respective security challenges
- Common vulnerabilities and threats specific to cloud environments and strategies for their prevention and mitigation
- Identity and access management (IAM) in cloud environments
- Authentication and authorization mechanisms for cloud services
- Principles of secure data storage and encryption in the cloud
- Network security in cloud environments, including VPNs and firewalls
- Best practices for securing AWS storage services such as Amazon S3 and Amazon EBS
- AWS security compliance programs and frameworks
- Incident response and disaster recovery in AWS environments
- **Microsoft Azure Security Concepts**
- Microsoft Cloud Adoption Framework for Azure
- Security measures to protect Azure resources such as virtual machines, databases, storage accounts, and networking components
- Identity and access controls management in Azure using Azure Active Directory (AAD), RBAC, and MFA
- Azure Virtual Network (VNet) and network security implementation
- Protecting data at rest and in transit using Azure security features
- Azure Key Vault for managing cryptographic keys, secrets, and certificates
- Microsoft Defender for Cloud to monitor and improve Azure security

- Security monitoring and logging in the cloud
- Incident response and disaster recovery strategies for cloud-based systems
- Best practices for securing cloud-based infrastructure and services
- Regulatory and compliance requirements related to cloud security
- Shared responsibility model and the division of security responsibilities between cloud providers and customers
- Knowledge of cloud security frameworks such as CSA (Cloud Security Alliance)
- **AWS Security Concepts**
- AWS shared responsibility model and security responsibilities division
- AWS Cloud Adoption Framework and its security capabilities
- Secure AWS identities and access management
- Configure and secure AWS networking components such as VPCs, subnets, and security groups
- AWS encryption mechanisms, including data-at-rest and data-in-transit encryption
- AWS monitoring and logging services including AWS CloudTrail and Amazon CloudWatch
- AWS security services such as AWS WAF, AWS Shield, and AWS Inspector

posture

- Azure Monitor, Azure Sentinel, and threat intelligence capabilities
- Azure governance frameworks and compliance management
- Incident response procedures and disaster recovery planning in Azure
- **Google Cloud Platform (GCP) Security Concepts**
- Google Cloud Adoption Framework
- GCP security concepts, tools, and services for protecting cloud-based resources
- Implement and configure IAM roles, policies, and permissions in GCP
- Design and configure secure virtual networks (VPCs) in GCP
- GCP network security tools such as Cloud Armor, Cloud VPN, and Cloud DNS
- Protect sensitive data using encryption and Google Cloud Key Management Service (KMS)
- Logging and monitoring using Google Cloud Security Command Center and Operations Suite Logging
- Secure application development on GCP and vulnerability management
- GCP compliance frameworks, certifications, and regulatory requirements
- Incident response planning and disaster recovery techniques in GCP

Prerequisites:

Attendees should meet the following pre-requisites:

- Should have a working knowledge of network security management
- Basic understanding of cloud computing concepts

Testing and Certification

Recommended as preparation for the following exam:

- **312-40 -** Certified Cloud Security Engineer **Examination**

Test Format
Multiple Choice

Number of Questions
125

Duration
4 Hours

Passing Score
70%

Availability
EC-Council Exam Portal

Content:

MODULE 01 : Introduction to Cloud Security

This module provides a basic understanding of cloud computing and its service models, including the various threats and vulnerabilities found in the cloud. It highlights various factors for evaluating service providers and understanding the shared security responsibility model of service providers. Understanding the shared responsibility model provided by the cloud service provider is essential to configuring the cloud environment securely and protecting organizational resources.

MODULE 02 : Platform and Infrastructure Security in the Cloud

This module explains the key components and technology that make the architecture of the cloud and the various techniques involved in securing the multi-tenancy, virtualized, physical, and logical cloud components. It demonstrates the configurations to secure the physical data center. Users can learn the best practices to secure the workload, computing resources, and networks in the cloud. This module demonstrates the use of various services and tools provided for network and computing security in Azure, AWS, and Google Cloud.

MODULE 03 : Application Security in the Cloud

This module focuses on securing cloud applications, from designing to deployment of an application in the cloud. It explains the changes in the Secure Software Development Life Cycle (SSDLC) in the cloud. It shows how service providers' identity and access management features help implement authentication and authorization and restrict unauthorized users from accessing cloud resources. It teaches the implementation of security controls throughout the software development life cycle. This module highlights integrating security into DevOps and the continuous integration/continuous deployment (CI/CD) model for developing and deploying cloud applications. This module demonstrates the use of various services and tools provided for application security in Azure, AWS, and Google Cloud.

MODULE 04 : Data Security in the Cloud

Data security is the major concern while

MODULE 05 : Operation Security in the Cloud

This module includes the security controls for building, implementing, operating, managing, and maintaining physical and logical infrastructure for cloud environments. It covers the services, features, and tools AWS, Azure, and Google Cloud provide for operational security.

MODULE 06 : Penetration Testing in the Cloud

This module demonstrates how to implement a comprehensive penetration testing methodology for assessing the security of an organization's cloud infrastructure. It demonstrates the various services and tools used to perform penetration testing in AWS, Azure, and Google Cloud.

MODULE 07 : Incident Detection and Response in the Cloud

An incident response (IR) plan is crucial to prevent security breaches in the cloud. This module describes the incident response life cycle and highlights the considerations for responders in each phase of the IR plan in a cloud environment. It highlights the use of SOAR in automating incident response in the cloud. This module explores the incident response capabilities provided by AWS, Azure, and Google Cloud. It demonstrates various tools and services for incident detection and response.

MODULE 08 : Forensics Investigation in the Cloud

Access to forensic data and the forensic investigation process in a cloud computing environment differ from the network forensic investigation process. This module highlights various cloud forensic challenges and data collection methodologies. It demonstrates how to investigate security incidents in the cloud using various tools provided by AWS, Azure, and Google Cloud.

MODULE 09 : Business Continuity and Disaster Recovery in the Cloud

Business Continuity and Disaster Recovery (BC/DR) is important in the cloud because a third party manages the resources. This module teaches the role of the business continuity and disaster recovery plan in the cloud. It explains backup and recovery tools and the services and features provided by service providers such as AWS, Azure, and Google Cloud to prepare and manage outages to ensure business continuity.

MODULE 10 : Governance, Risk Management, and Compliance in the Cloud

This module highlights the standards, policies, and legal issues related to the cloud. It highlights various legal and compliance issues found in a cloud environment. It discusses various cloud security standards and audit planning in the cloud. It demonstrates the features, services, and tools for compliance and auditing in Azure, AWS, and Google Cloud.

MODULE 11 : Standards, Policies, and Legal Issues in the Cloud

This module highlights the standards, policies, and legal issues related to the cloud. It highlights various legal and compliance issues found in a cloud environment. It discusses various cloud security standards and audit planning in the cloud. It demonstrates the features, services, and tools for compliance and auditing in Azure, AWS, and Google Cloud.

migrating to the cloud. This module covers the basics of cloud data storage, its life cycle, and various controls to protect data-at-rest and data-in-transit in the cloud. This module includes data storage features and various services and tools for securing the data stored in Azure, AWS, and Google Cloud.

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo