EC-Council Certified Cloud Security Engineer (C|CSE) + Exam voucher

Duration: 5 Days **Course Code: ECCCSE** **Version: 1.0**

Overview:

Certified Cloud Security Engineer (C|CSE) is a specialized program curated by cloud security professionals in collaboration with subject matter experts from across the globe. A hands-on learning certification course, CICSE adopts a detailed and methodological approach to teaching fundamental cloud security concepts.

EC Council's C|CSE program is a blend of vendor-neutral and vendor-specific cloud security concepts that offer aspirants an unbiased learning approach. Vendor-neutral concepts emphasize universally applicable cloud security best practices, technology, and frameworks that help individuals strengthen their fundamentals. Vendor-specific concepts help individuals gain the practical skills they need to work with a specific cloud platform.

The C|CSE certification program offers the following features:

C|CSE is a unique course that stands apart from other cloud computing programs.
It offers comprehensive knowledge and practical learning for security practices, tools, and techniques used to configure widely used public cloud providers such as Amazon Web Services (AWS), Azure, and GCP.
It enables candidates to learn the necessary skills required in real-world threat scenarios from industry experts.
C|CSE plays an active role in enhancing an organization's security posture by training professionals to plan, configure, implement, and maintain a secure cloud environment.
It prepares participants to protect, detect, and respond to threats in the cloud network.

Target Audience:

Anyone working in a cloud environment who need to expand and develop their cloud security skills and knowledge.

Objectives:

- **After completing this course you should be able to:**
- Plan, implement, and execute cloud platform security for an organization.
- Evaluate and mitigate security vulnerabilities, risks, and threats in a cloud platform.
- Securely access cloud resources through 1AM.
- Integrate best practices to secure cloud infrastructure components (network, storage and virtualization, and the management plane).
- Evaluate and control organizational cloud network architecture by integrating various security controls the service provider offers.
- Secure organizational cloud applications by understanding the secure software development lifecycle of cloud applications and implementing additional security controls to enhance the security of the hosted cloud applications.
- Evaluate cloud storage techniques and threats on the data stored in the cloud and understand how to protect cloud data from attacks.
- Design and implement a GRC framework for the organizational cloud infrastructure by evaluating various compliance frameworks and understanding the compliance features provided by the service provider.
- Implement and manage cloud security on various cloud platforms such as AWS, Azure, and Google Cloud Platform.
- Utilize the security services and tools provided in Azure, AWS, and Google Cloud to secure the organizational cloud environment by understanding the shared responsibility model of the service provider.
- Understand the legal implications associated with cloud computing to prevent organizations from legal issues.
- Evaluate various cloud security standards and organizations responsible for providing these standards.
- Perform cloud computing security audits and penetration testing to help organizations follow the standards, policies, procedures, and regulations governing cloud environments.
- Understand and evaluate the various compliance programs and features offered by AWS, Azure, and Google Cloud.
- Implement operational controls and standards to build, operate, manage, and maintain the cloud infrastructure.
- Implement the various threat detecting and responding services provided by Azure, AWS, and Google cloud to indentify threats to the organizational cloud services.
- Understand and implement security for private, multi-tenant and hybrid cloud environments.

- Design and implement a cloud incident response plan for the organization and detect security incidents using security automation tools.
- Design and implement a business continuity plan for cloud services by implementing end-to-end backup and recovery solutions.
- Learn to secure multi-cloud and hybrid computing environments.

Prerequisites:

Attendees should meet the following pre-requisites:

- Have working knowledge in 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

Content:

Introduction to Cloud Security

This module presents the core concepts of cloud computing, cloud service models, and cloud-based threats and vulnerabilities. It highlights service provider components, such as evaluation and the shared security responsibility model, which are essential to configuring a secure cloud environment and protecting organizational resources.

Module 02: Platform and Infrastructure Security in Cloud

Learn the key components and technologies that build cloud architecture, such as securing the multi-tenancy, virtualized, physical, and logical cloud components. This module demonstrates configurations and best practices to secure the physical data center and cloud infrastructure utilizing tools and techniques provided by Azure, AWS, and Google Cloud.

Module 03: Application Security in Cloud

This module has a key focus on securing cloud applications and explains Secure Software Development Lifecycle (SSDLC) changes. It discusses multiple services and tools for application security in Azure, AWS, and Google Cloud.

Module 04: Data Security in Cloud

This module covers the basics of cloud data storage, its lifecycle, and various controls to protect data in rest and data in transit in the cloud, as well as data storage features and multiple services and tools used for securing the data stored on Azure, AWS, and Google Cloud.

Module 05: Operation Security in Cloud

This module focuses on the security controls that are essential to build, implement, operate, manage, and maintain the physical and logical infrastructure for cloud environments and the required services, features, and tools provided for operational security by AWS, Azure, and Google Cloud.

Module 06: Penetration Testing in Cloud

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

Module 07: Incident Detection and Response in Cloud

This module focuses on incident response (IR) and examines the incident response lifecycle, alongside tools and techniques used to identify and respond to incidents. It provides SOAR training and explores IR capabilities provided by AWS, Azure, and Google Cloud Platform.

Module 08: Forensics Investigation in Cloud

This module explores the forensic investigation process in cloud computing, various cloud forensic challenges, and data collection methods. It also illustrates the process of investigating security incidents using tools in AWS, Azure, and Google Cloud.

Module 09: Business Continuity and Disaster Recovery in Cloud

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

Module 10: Governance, Risk Management, and Compliance (GRC) in Cloud

This module focuses on various governance frameworks, models, and regulations (ISO-IEC 27017, HIPAA, and PCI DSS) and the designing and implementation of governance frameworks in the cloud. It also includes cloud compliance frameworks and elaborates on AWS, Azure, and Google Cloud governance modules.

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

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

Self-Study Appendices:

Private, Hybrid, and Multi-Tenant Cloud Security - These three appendices explore the security of private, hybrid, and multi-tenant cloud models. They reveal some of the best practices for securing VMWare cloud, AWS, GCP, Azure hybrid cloud setup, and multi-tenant 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