EC-Council CCSE: Certified Cloud Security Engineer

Category: Networking & Security | **Vendor:** EC-Council

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Cloud Security Engineer (CCSE)
Related Exam:	CCSE

Course 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.

About This Course

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.

Who Should Attend

- Network Security Administrator
- Network Security Engineer
- Network Security Analyst
- Cybersecurity Engineer
- Cybersecurity Analyst
- Cloud Administrator
- Cloud Engineer
- Cloud Analyst
- InfoSec professionals
- CND Certified professionals
- OR any other role that involves network/cloud administration, management, and operations

Prerequisites & Entry Requirements

General Prerequisites:

To be eligible to challenge the EC-Council C|CSE certification examination, candidate should:

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Plan, implement, and execute cloud platform security for an organization
- Securely access cloud resources through identity and access management (IAM)
- Evaluate and control organizational cloud network architecture by integrating various security controls the service provider offers
- Evaluate cloud storage techniques and threats on data stored in the cloud and understand how to protect cloud data from attacks
- Implement and manage cloud security on various cloud platforms, such as AWS, Azure, and GCP
- Understand the shared responsibility model of the service provider
- Evaluate various cloud security standards, compliance programs, and features offered by AWS, Azure, and GCP, and perform cloud computing security audits
- Implement various threat detection and response services provided by Azure, AWS, and GCP to identify threats to an organization's cloud services
- Evaluate and mitigate security risks, threats, and vulnerabilities in a cloud platform
- Integrate best practices to secure cloud infrastructure components (network, storage and virtualization, and management)
- Secure organizational cloud applications by understanding the secure software development lifecycle of cloud applications and by implementing additional security controls to enhance the security of hosted cloud applications
- Design and implement a GRC framework, a cloud incident response plan, and a business continuity plan for cloud services
- Utilize the security services and tools provided in Azure, AWS, and GCP to secure the organizational environment
- Understand the legal implications associated with cloud computing to protect organization
- Implement operational controls and standards to build, operate, manage, and maintain the cloud infrastructure
- Understand and implement security for private, multi-tenant, and hybrid cloud environments

Detailed Course Outline

- 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 migrating to the cloud. This module covers the basics of cloud data storage, its life cycle, and various controls to protect data-in-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.

- 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.

🎓 Certification Path

Certified Cloud Security Engineer (CCSE)

Exam: CCSE

Skills You Will Learn:

- Plan, implement, and execute cloud platform security for an organization
- Securely access cloud resources through identity and access management (IAM)
- Evaluate and control organizational cloud network architecture by integrating various security controls the service provider offers
- Evaluate cloud storage techniques and threats on data stored in the cloud and understand how to protect cloud data from attacks
- Implement and manage cloud security on various cloud platforms, such as AWS, Azure, and GCP
- Understand the shared responsibility model of the service provider
- Evaluate various cloud security standards, compliance programs, and features offered by AWS, Azure, and GCP, and perform cloud computing security audits
- Implement various threat detection and response services provided by Azure, AWS, and GCP to identify threats to an organization's cloud services
- Evaluate and mitigate security risks, threats, and vulnerabilities in a cloud platform
- Integrate best practices to secure cloud infrastructure components (network, storage and virtualization, and management)
- Secure organizational cloud applications by understanding the secure software development lifecycle of cloud applications and by implementing additional security controls to enhance the security of hosted cloud applications
- Design and implement a GRC framework, a cloud incident response plan, and a business continuity plan for cloud services
- Utilize the security services and tools provided in Azure, AWS, and GCP to secure the organizational environment
- Understand the legal implications associated with cloud computing to protect organization
- Implement operational controls and standards to build, operate, manage, and maintain the cloud infrastructure
- Understand and implement security for private, multi-tenant, and hybrid cloud environments

Frequently Asked Questions

Q: What delivery options are available for EC-Council CCSE: Certified Cloud Security Engineer?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The EC-Council CCSE: Certified Cloud Security Engineer course helps prepare you for the Certified Cloud Security Engineer (CCSE) certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the CCSE official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day EC-Council CCSE: Certified Cloud Security Engineer course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council CCSE: Certified Cloud Security Engineer training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council CCSE: Certified Cloud Security Engineer?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council CCSE: Certified Cloud Security Engineer. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: EC-Council Certified Cloud Security Engineer, Specialist, CCSE

Q: Why choose Nexus Human for EC-Council CCSE: Certified Cloud Security Engineer?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council CCSE: Certified Cloud Security Engineer training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 19/10/2026.