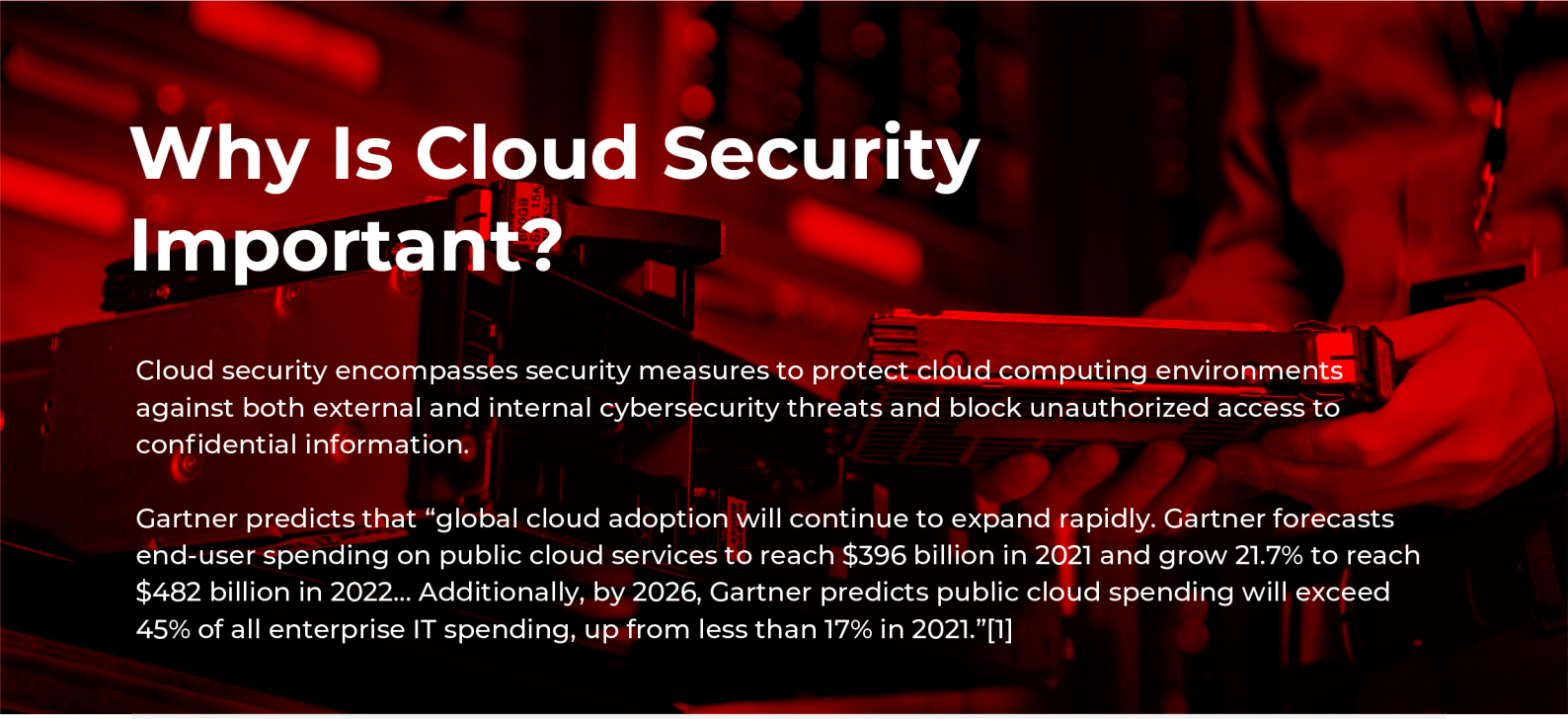
EC-Council

C|CSE
Certified Cloud Security Engineer

Certified Cloud Security Engineer (C|CSE) Course

Cloud Security is a Crucial Component in Reducing Risks and Maintaining Compliance Regulations in Cloud Computing.

Master Cloud Security Implementation and Management with a first of its kind certification that is both vendor neutral and vendor specific.



Why Is Cloud Security Important?

Cloud security encompasses security measures to protect cloud computing environments against both external and internal cybersecurity threats and block unauthorized access to confidential information.

Gartner predicts that "global cloud adoption will continue to expand rapidly. Gartner forecasts end-user spending on public cloud services to reach $396 billion in 2021 and grow 21.7% to reach $482 billion in 2022... Additionally, by 2026, Gartner predicts public cloud spending will exceed 45% of all enterprise IT spending, up from less than 17% in 2021."[1]

Cloud infrastructure facilitates seamless storage and data exchange, enhanced productivity and reliability, and reduced operational and overhead costs for organizations. However, despite the benefits, migrating to the cloud exposes enterprises to security threats, including data loss, unsecured APIs, and data breaches. All of these threats have increased in recent years, partly due to the use of the public cloud to store enterprises' critical and sensitive client and business data. With more enterprises shifting to the cloud, security concerns are at an all-time high.

Around **36%** of organizations have experienced a major cloud security data breach in the past 12 months.[2]

Approximately **64%** of organizations feel the problem will only escalate or remain unchanged in the next 12 months.[3]

Misconfiguration of the cloud platform is one of the primary factors contributing to cloud breaches. Every cloud platform has a distinct set of legal policies, compliance, and regulatory standards. Organizations often use multi-cloud platforms, which necessitates the presence of skilled professionals who can resolve any issues.

Cloud security helps organizations by:

1. Protecting the organization's security posture.
2. Securing cloud environments against unauthorized use/access.
3. Protecting a client's privacy on the cloud.
4. Minimizing DoS attacks.
5. Maintaining regulatory compliance.

Maintaining cloud security protocols is a shared responsibility between the cloud service provider and the user. Understanding the cloud shared responsibility model is essential for both the cloud provider and the user as they are accountable for different security components and must work together to safeguard their resources.

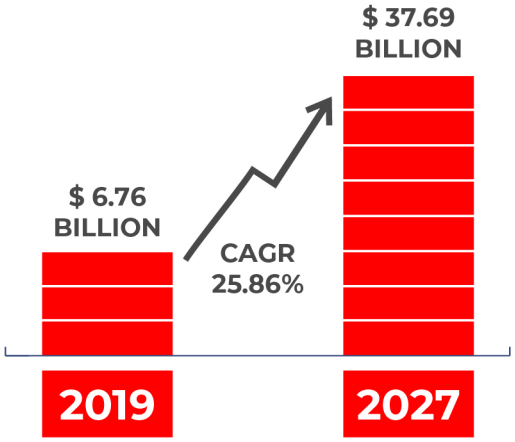
[1] - https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

[2] - https://resources.fugue.co/state-of-cloud-security-2021-report

[3] - https://digitalisationworld.com/news/61996/third-of-businesses-suffered-a-serious-cloud-data-breach-or-leak-as-hackers-exploit-misconfigurations

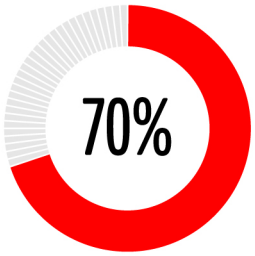
Cloud Security – An In Demand Cybersecurity Skill In 2021

Post COVID-19, the cloud security market is expected to grow at a Compound Annual Growth Rate (CAGR) of 25.86% from USD 6.76 billion to USD 37.69 billion by 2027.[4]

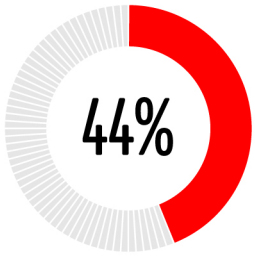


While the demand for cloud security professionals is high, the talent drought in the field is alarming. There are several contributing factors to the cloud security skills shortage:

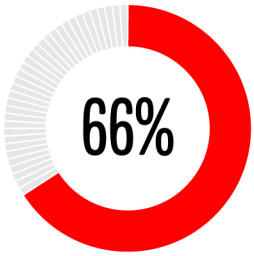
1. The absence of specialized professionals equipped with the latest technical skills and resources to handle cloud complexities.
2. A lack of awareness among enterprises to train their security personnel to meet specific cloud security needs.
3. Most companies don't want to invest in cloud security talent pools.



of enterprises relying on public cloud to run their businesses have suffered security incidents[5]



of businesses anticipate security challenges from data theft or loss



of organizations suffer from the consequences of misconfiguration of cloud servers

EC-Council has launched a comprehensive Certified Cloud Security Engineer (CCSE) program to meet the increasing demand for cloud security professionals. This specialization equips individuals with in-demand skills associated with the cloud and will help organizations build a robust in-house cloud security team.

[4] - https://www.verifiedmarketresearch.com/product/global-cloud-security-market-size-and-forecast-to-2025/

[5] - https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

Earn the C|CSE Certification and Master the Skills to Secure Critical Assets in the Cloud

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, C|CSE 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 infrastructure through distinctive online training options.

How Does C|CSE Address Cloud Security Concerns?

With the increasing complexity of cyberattacks, a reactive approach alone is not sufficient. Since dealing with the aftermath of a cloud security breach can be a daunting scenario, organizations need to stay ahead of the attacks to stay protected. A single incident can have far-reaching consequences, necessitating the presence of experts who have in-depth knowledge of cloud infrastructure and the challenges associated with it. The C|CSE curriculum was crafted to address the challenges organizations face in ensuring cloud security and to enable candidates to become job ready.

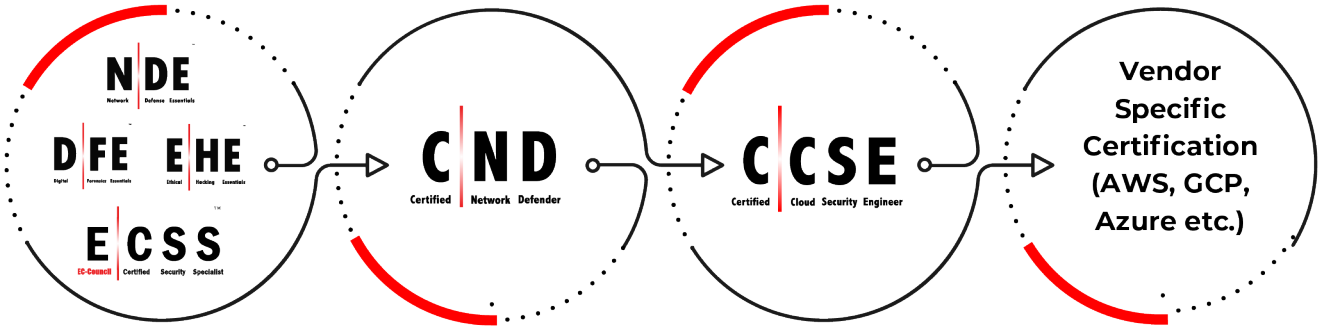
Industry Challenges	How Can C|CSE Help
While organizations believe that it is the responsibility of the cloud service providers (CSPs) to safeguard their data, one the other hand, CSPs consider it to be a shared responsibility.	The curriculum explores the core concepts of cloud computing, cloud service models, and cloud-based vulnerabilities. It discusses the service provider components in detail, such as evaluation and the shared responsibility model to safeguard an organization's resources.
As more organizations migrate to the cloud, there is a rising demand for cloud security professionals who are equipped with the right skills.	The C|CSE course equips candidates with the necessary skills to protect, detect, and respond to cloud security attacks through extensive modules, making them industry ready.
Because many organizations use multi-cloud platforms, they need professionals with multi-cloud security expertise.	The course demonstrates how tools, techniques, and procedures can be employed on major and widely used public cloud service providers (AWS, Azure, GCP) through vendor-neutral and vendor-specific training. While vendor-neutral training teaches candidates cloud fundamentals, vendor-specific training helps individuals acquire the skills required to work with specific cloud platforms.
Ensuring legal, compliance, and regulatory standards in organizations using multi-cloud platforms can be a difficult task requiring expertise in the domain.	EC-Council's C|CSE program offers a dedicated module on the legal policies, compliance, and regulatory standards applicable to the AWS, Azure, and GCP cloud environments.
Misconfiguration of the cloud platform or wrong setup is one of the primary loopholes leading to security breaches.	The course discusses various mitigation techniques for the possible misconfiguration across the AWS, Azure, and GCP cloud platforms to secure the multi-tenancy, virtualized, logical, and physical cloud components.
Improperly secured cloud control plane can lead to data loss, regulatory fines, and more.	The curriculum imparts vital information about application and data security in cloud environments to prevent tarnishing an organization's credibility and reputation and the subsequent revenue loss.

Who Is It For?

This course is intended for professionals who work as:

- Network security administrator/engineers/analysts
- Cybersecurity engineers/analysts
- Cloud administrators/analysts/engineers
- CND-certified professionals
- Any other role that involves network administration, cloud administration, management, and operations
- Information security professionals

Career Progression to Cloud Security



Why Choose C|CSE?

Data breaches are a threat to the operations of any organization. It pays to invest in building an in-house team of cloud security engineers who are adept at handling cloud infrastructure complexities. EC-Council is one of the few ANSI 17024 accredited institutions globally specializing in information security. The course framework for the C|CSE certification by EC-Council is designed and developed by industry practitioners in collaboration with subject matter experts. The certification program is beneficial for both individuals and organizations.

How does it benefit individuals?

- Offers a simulated environment with 50+ complex labs to equip candidates with skills that matter to make them job ready
- Mapped with real-time job roles and responsibilities of cloud security professionals
- A one of its kind program offering vendor-neutral and vendor-specific cloud security concepts
- Covers security implementation practices for widely used public cloud service providers, such as AWS, Azure, and GCP
- Furnished with best practices to perform forensics activities across various cloud platforms, such as AWS, Microsoft Azure Cloud, and Google Cloud Platform
- Candidates learn real-world job skills in a hands-on lab environment that equips them with the expertise and responsibilities required of cloud security professionals.

How does it benefit organizations?

- Organizations can build an in-house team of cloud security professionals. Upskilling their existing talent pool on cloud technologies can help them save time and resources compared to hiring and training new recruits.
- With its unique blend of vendor-neutral and vendor-specific cloud security concepts, C|CSE helps organizations leverage candidates' expertise in multi-cloud environments.
- The C|CSE program teaches students to design and implement business continuity and disaster recovery plans for the cloud.
- Hands-on practice teaches candidates how to perform cloud computing security audits and penetration testing to help organizations comply with the standards, policies, procedures, and regulations governing cloud environments.

Course Outline

Module 01: 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.

What Will You Learn?

After attending this cloud security course, participants will 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 IAM.
- 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.
- 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.
- 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 identify threats to the organizational cloud services.
- Understand and implement security for private, multi-tenant, and hybrid cloud environments.
- Learn to secure multi-cloud and hybrid cloud computing environments.

C|CSE Training Information

Training Duration:	**5 Days**
Training Timing:	**9:00 AM to 5:00 PM**
Delivery Mode:	• **Instructor-led training** • **iWeek (synchronous online learning)** • **iLearn (asynchronous online learning)**

C|CSE Exam Details

Exam Title:	**Certified Cloud Security Engineer**
Exam Code:	**312-40**
Number of Questions:	**125**
Duration:	**4 hours**
Availability:	**EC-Council Exam Portal**
Test Format:	**Multiple Choice**

Recommended Prerequisites

- Have working knowledge in network security management.
- Basic understanding of cloud computing concepts.

About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. The organization helps individuals, companies, educators, and governments address global workforce problems through the development and curation of world-class cybersecurity education programs and their corresponding certifications. EC-Council also provides cybersecurity services to some of the largest businesses around the world. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the global intelligence community, NATO, and more than 2,000 of the best universities, colleges, and training companies, EC-Council programs have proliferated through more than 140 countries and have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker program, EC-Council is dedicated to equipping more than 230,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, and the Certified Chief Information Security Officer program, among others. EC-Council is an ANSI 17024 accredited organization and has earned recognition by the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and a variety of other authoritative bodies that influence the entire profession. Founded in 2001, EC-Council employs over 400 people worldwide with 10 global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL. Learn more at www.eccouncil.org

© 2021 EC-Council. All rights reserved. EC-Council and C|CSE logos are registered trademarks or trademarks of EC-Council in the United States and/or other countries.