A First of its kind
Vendor Neutral and
Vendor Specific Certification

EC-Council
eHACK ACADEMY

The **Next Dimension** in Cloud Computing

Certified Cloud Security Engineer (C|CSE)

Become a complete Cloud Security Expert

www.eccouncil.org

What is **Cloud Security,** and why is it **Important?**

Enterprise IT spending on public cloud technologies is expected to jump from under 17% of expenditures in 2021 to over 45% by 2026 (Gartner, 2021). According to the same report, the public cloud service market is expected to reach USD 482 billion by the end of 2022.

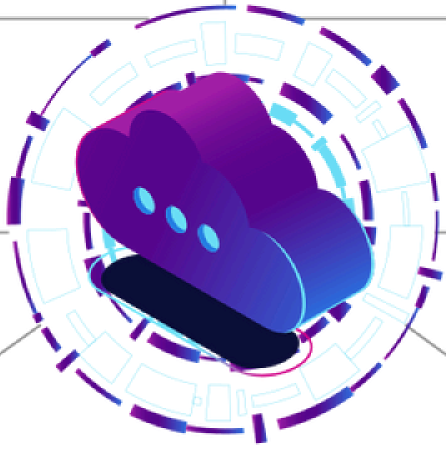
Cloud infrastructures facilitate seamless storage and data exchange, enhance productivity and reliability, and reduce operational and overhead costs for organizations. Despite these benefits, migrating to the cloud can expose enterprises to a variety of security threats, including data loss, unsecured APIs, and data breaches. These threats have increased in recent years, due in part to the use of public clouds to store enterprises' critical client and business data. With a growing number of enterprises shifting to the cloud, security concerns are at an all-time high.

Cloud security is the practice of protecting cloud-based infrastructure, data, and applications. It is a series of principles, methodologies, and technologies designed to control and secure cloud environments.

Today, 92% of organizations' IT environments are located at least partially in the cloud (IDG, 2020).

65% of cloud network security breaches occur as a result of user error (Nunnikhoven, 2021).

Roughly 36% of organizations experienced a major cloud security data breach in the past year (Fugue, 2021)



Migrating to the public cloud can cut your total cost of ownership up to 40% (Lacy et al., 2020).

On average, a cloud outage lasts 117 minutes—almost two hours (Veeam, 2020).

Over 33B records have been exposed over the last two years (Greig, 2020).

The average cost of a cloud security breach is USD 5.12M (IBM, 2021).

Top Cloud Security Challenges

- Controlling cloud costs
- Ensuring data privacy and security
- Securing and protecting cloud resources
- Lack of cloud security skill/ expertise
- Implementing governance and compliance

Fugue: (2021). The state of cloud security 2021.

Gartner: (2021, August 2). Gartner says four trends are shaping the future of public cloud [Press release].

Greig, J: (2020, February 20). Cloud misconfigurations cost companies nearly $5 trillion. TechRepublic.

IBM: (2021). Cost of a data breach: A view from the cloud 2021.

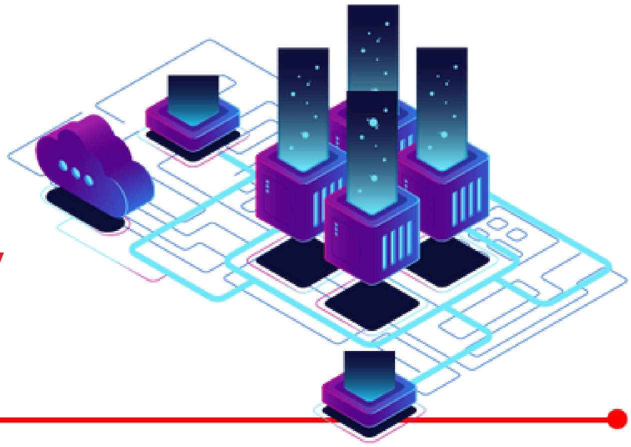
GrIDG: (2020). 2020 IDG cloud computing study [Executive summary].

Lacy, P., Daugherty, P., Ponomarev, P., & Durg, K: (2020). The green behind the cloud. Accenture.

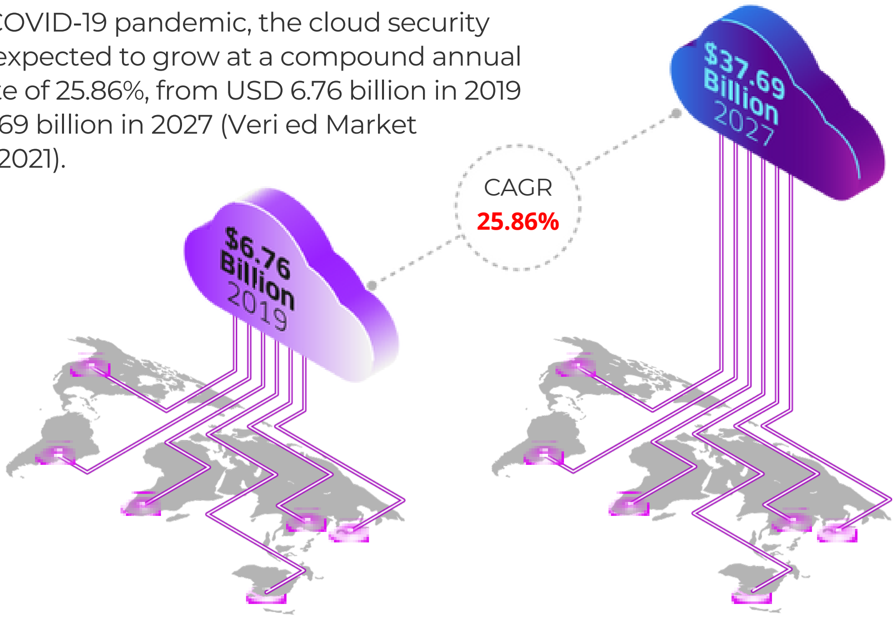
Nunnikhoven, M: (2021, January 13). The top worry in cloud security for 2021. Trend Micro.

Veeam: . (2020, June 2). CXO research: Legacy technology and lack of skills hindering digital transformation and IT modernization [Press release].

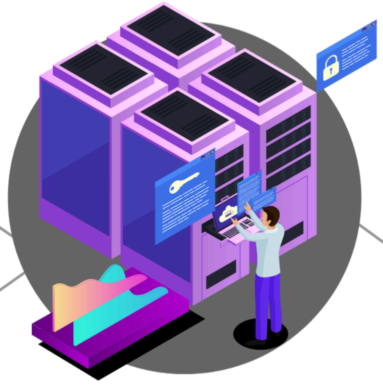
Cloud Security:
An In-Demand **Cybersecurity Skill** in 2022 and **Beyond**



After the COVID-19 pandemic, the cloud security market is expected to grow at a compound annual growth rate of 25.86%, from USD 6.76 billion in 2019 to USD 37.69 billion in 2027 (Verified Market Research, 2021).



The talent drought in this field is alarming given the high demand for cloud security professionals. Several factors contribute to the cloud security skills shortage:



There is a lack of specialized professionals equipped to handle cloud complexities with the most up-to-date technical skills and resources.

Most companies do not want to invest in cloud security talent pools.

Enterprises lack the necessary knowledge to train their personnel to meet specific cloud security needs.

70%
% of enterprises relying on the public cloud to run their businesses have suffered security incidents

44%
of businesses anticipate experiencing security challenges resulting from data theft or loss (Sophos, 2020).

66%
of organizations have suffered the consequences of misconfiguring cloud servers (Sophos, 2020).

EC-Council has launched a comprehensive Certified Cloud Security Engineer (C|CSE) program to meet the increasing demand for cloud security professionals. This specialization equips individuals with in-demand cloud security skills and helps organizations build robust in-house cloud security teams.

Sophos: (2020). The state of cloud security 2020.

Verified Market Research: . (2021). Cloud security market size and forecast.

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

EC-Council's **Certified Cloud Security Engineer** (C|CSE) course is a specialized program curated by cloud security professionals in collaboration with subject matter experts from around the globe. C|CSE is a hands-on learning certification course that adopts a detailed and methodological approach to teaching the fundamental concepts of cloud security.

EC-Council's C|CSE program blends vendor-neutral and vendor-specific cloud security concepts, offering aspirants an unbiased learning approach. Vendor-neutral concepts emphasize universally applicable cloud security best practices, technologies, and frameworks to help individuals strengthen their grasp of the fundamentals. Vendor-specific concepts help individuals gain the practical skills needed to work with specific cloud platforms.

Why Choose C|CSE? and Benefits of C|CSE

C|CSE is a unique course that stands apart from other cloud computing programs.

Offers comprehensive knowledge and practical learning of security practices, tools, and techniques used to configure widely used public cloud providers such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP)

Enables you to learn the skills required in real-world threat scenarios from industry experts

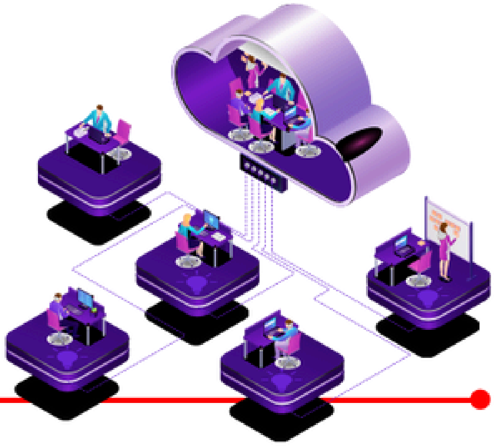
Plays an active role in enhancing your organization's security posture by teaching you how to plan, configure, implement, and maintain a secure cloud environment

Demonstrates how to perform cloud computing security audits and penetration testing to help organizations comply with the standards, policies, procedures, and regulations governing cloud environments

Provides a simulated environment with over 50 complex labs to equip you with skills that matter and ensure job readiness

Is mapped with real-time job roles and responsibilities of cloud security professionals

Who is it for?



This course is intended for professionals working as:

Network Security administrators, engineers, and analysts

Cybersecurity engineers and analysts

Cloud administrators, engineers, and analysts

CND Certified professionals

InfoSec professionals

Any other role involving **network and cloud administration, management** and **operation**

Career Progression to Cloud Security

E|CSS

EC-Council Certified Security Specialist

& Essentials

N|DE Network Defense Essentials

E|HE Ethical Hacking Essentials

D|FE Digital Forensics Essentials

▶ C|ND

Certified Network Defender

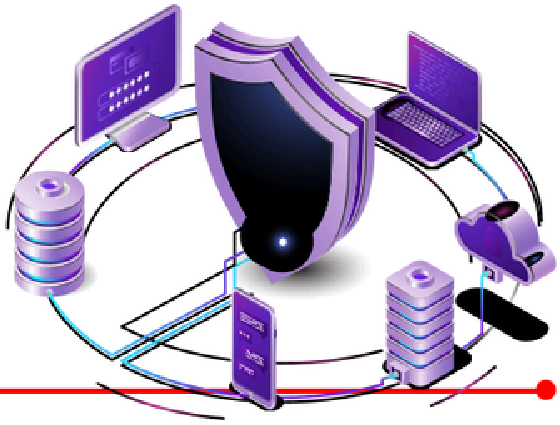
▶ C|CSE

Certified Cloud Security Engineer

▶ **Vendor Specific Certification**

(AWS, GCP, Azure, etc.)

How does C|CSEAddress **Cloud Security** Concerns?



With the increasing complexity of cyberattacks, a reactive approach alone is insufficient. Dealing with the aftermath of a cloud security breach can be daunting, and organizations need to stay ahead of attacks to remain protected. A single incident can have far-reaching consequences, necessitating the presence of experts with in-depth knowledge of cloud infrastructure and associated challenges. The C|CSE curriculum was crafted to address the challenges organizations face in ensuring cloud security and enabling candidates to become job ready.

Industry Challenges	How C|CSE Helps
Cloud security is a shared responsibility	Provides a detailed discussion of service provider components needed to safeguard an organization's resources, such as evaluation and the shared responsibility model
High demand for cloud security professionals with specialized skills	Equips candidates with the skills necessary to protect, detect, and respond to cloud security attacks through extensive modules, making them industry ready
Organizations leveraging multi-cloud solutions require professionals with multi-cloud security expertise	Demonstrates tools, techniques, and procedures employed by major and widely used public cloud service providers (AWS, Azure, and GCP) through vendor-neutral and vendor-specific training
Need to adhere to legal, compliance, and regulatory standards in organizations using multi-cloud platforms	Presents legal policies, compliance issues, and regulatory standards applicable to the AWS, Azure, and GCP environments
Increase in cloud security breaches	Examines various mitigation techniques for possible misconfigurations across the AWS, Azure, and GCP environments to secure multi-tenant, virtualized, logical, and physical cloud components
Data privacy and security challenges	Imparts vital information about application and data security in cloud environments to prevent tarnishing of an organization's credibility and reputation and subsequent revenue loss

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.

Course Outline

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.

Common**Job Roles**

- Cloud Security Engineer
- Cloud Security Consultant
- Cyber Cloud Security Manager
- Cloud Security Architect
- Cloud Security Manager
- API Cloud Security Engineer
- Cloud Security Technical Lead
- Cloud Security Administrator
- Cloud Security Analyst
- Cloud Security Specialist
- IT Delivery Manager - Cloud Security Engineer
- Cloud Security and Compliance Specialist
- Cloud Security Operations Lead
- Cloud Security Practice Manager
- Cloud Security Engineer - DevSecOps
- DevSecOps Cloud Security Architect
- Cloud Security/OPS
- Cloud Security SME
- Cloud Security Project Manager
- Cloud Security/Operations Engineer
- Cloud Security/Infosec/SecOps Engineer
- Clouds DevOps Engineer

C|CSE Training, Exam Details and About **EC-Council**

C|CSE Training Information

Training Duration	: 5 days
Training Timing	: 9 a.m. – 5 p.m.
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. We help individuals, organisations, educators, and governments address global workforce problems through the development and curation of world-class cybersecurity education programmes and their corresponding certifications and provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programmes have proliferated through over 140 countries and have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programme, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organisation cyber capabilities through the Certified Ethical Hacker Programme, followed by a variety of other cyber programmes, 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, as well as the Certified Chief Information Security Officer. We are an ANSI 17024 accredited organisation and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST and various other authoritative bodies that influence the entire profession. Founded in 2001, EC-Council employs over 400 individuals 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

EC-Council

www.eccouncil.org

/ECCouncil /company/ec-council /ECCOUNCIL /user/eccouncilusa