CYBER SECURITY

EC-Council Certified Cloud Security Engineer

INCLUSIONS	LENGTH	VERSION
Exam voucher	**5 days**	**1**

EC-COUNCIL AT LUMIFY WORK

The International Council of E-Commerce Consultants (EC-Council) is a member-based organisation that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) and Licensed Penetration Tester (LPT) certifications and cyber security courses. Lumify Work is the partner of choice for EC-Council in Australia.

WHY STUDY THIS COURSE

EC-Council's Certified Cloud Security Engineer (CCSE) course is a specialised program curated by cloud security professionals in collaboration with subject matter experts from around the globe. CCSE 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 CCSE program blends vendor-neutral and vendor-specific cloud security concepts, offering aspirants an unbiased learning approach. Vendor-neutral concepts emphasise 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.

Exam vouchers
Note that exams are not taken while sitting an EC-Council course. You will be provided with an exam voucher. Candidates are required to book their exam after completion of the course, and are welcome to book a spot at their local Lumify Work campus. Your voucher will come with an expiry date. Please refer to the Lumify Work booking terms and conditions regarding exam voucher validity.

WHAT YOU'LL LEARN

- Fundamental cloud security concepts including IAM, encryption, key management, and password management
- The shared security responsibility models, features, and control evaluation of cloud service providers
- Security management of the cloud platform (PaaS), infrastructure (IaaS), and software (SaaS) platforms
- Cloud data security

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/

CYBER SECURITY

EC-Council Certified Cloud Security Engineer

- Cloud operation security, i.e., monitoring the security of the cloud
- Cloud penetration testing, its scope, and legal permissions
- Incident detection and response in cloud environment
- Cloud forensics and challenges
- Disaster recovery and business continuity for cloud environments
- Vendor specific Cloud standards, compliance, policies, and legal issues

My instructor was great being able to put scenarios into real world instances that related to my specific situation.

I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.

Great job Lumify Work team.

AMANDA NICOL
IT SUPPORT SERVICES MANAGER - HEALTH WORLD LIMITED

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/

CYBER SECURITY

EC-Council Certified Cloud Security Engineer

COURSE SUBJECTS

Refer to the CCSEv1 Outline for a deeper dive into the CCSE curriculum.

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 conjuring a secure cloud environment and protecting organisational resources.

Module 02. Platform and Infrastructure Security in Cloud
This module explores the key components and technologies that form a cloud architecture and how to secure multi-tenant, virtualised, physical, and logical cloud components. This module demonstrates congurations 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 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 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. Security Operations in 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 Cloud
This module demonstrates how to implement comprehensive penetration testing to assess the security of an organisation's cloud infrastructure and reviews the required services and tools used to perform penetration testing in AWS, Azure, and GCP.

Lumify Work Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.

For more information, please contact us on 02 8286 9429.

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/

CYBER SECURITY

EC-Council Certified Cloud Security Engineer

Module 07. Incident Response in 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. Forensic Investigation in 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 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 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 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.

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/

CYBER SECURITY

EC-Council Certified Cloud Security Engineer

WHO IS THE COURSE FOR?

- Network security administrator/engineer/analyst
- Cyber security engineer/analyst
- Cloud administrator/analyst/engineer
- CND certified professionals
- Info Security Professionals
- Any other role that involves network/cloud administrations, management, and operations

We can also deliver and customise this training course for larger groups – saving your organisation time, money and resources. For more information, please contact us via email on ph.training@lumifywork.com

PREREQUISITES

IT Security and Cloud experience is strongly recommended.

This course is suitable for the following job roles:

- Network security administrators, network security engineers, network defenders, cybersecurity engineers, and any other job role that involves handling the security of traditional network environments.
- Cloud administrators, cloud engineers, and other industry professionals with experience in managing cloud platforms.
- Any other role that involves network or cloud administration, management, and operations.

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/

CYBER SECURITY

EC-Council Certified Cloud Security Engineer

https://www.lumifywork.com/en-ph/courses/ec-council-certified-cloud-security-engineer/