CCSE – Certified Cloud Security Engineer

EC-Council

- **Nível:** Avançado
- **Duração:** 40h

Sobre o curso

EC-Council's Certified Cloud Security Engineer (CCSE) 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.

Download the brochure

Why Should You Become a Certified Cloud Security Engineer (CCSE)?

Organizations need cloud security engineers to help them build a secure cloud infrastructure, monitor vulnerabilities, and implement incidence response plans to mitigate cloud-based threats. CCSE, with its unique blend of vendor-neutral and vendor-specific concepts, trains candidates in the fundamentals while equipping them with job-ready practical skills. With CCSE, candidates learn:

01 – The fundamentals of cloud security in a vendor-neutral environment

---

02 – How to use tools and techniques to configure public cloud providers such as AWS, Azure, and GCP

03 –How to design and maintain a secure cloud environment

04 – The knowledge and skills to protect, detect, and respond to cloud network infrastructure threats

05 – How to design and implement business continuity and disaster recovery plans

06 – How to perform a cloud security audit and penetration testing

Destinatários

Who Should Earn a Cloud Security Certification?

- Network security engineers
- Cybersecurity analysts
- Network security analysts
- Cloud administrators and engineers
- Network security administrators
- Cloud analysts
- Cybersecurity engineers
- Those working in network and cloud management and operations

Objetivos

- 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 cloud environment.
- Understand the legal implications associated with cloud computing to protect organizations.
- 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.

Condições

O exame EC-Council incluido no valor do curso deve ser obrigatoriamente realizado presencialmente, num dos centros de Exames GALILEU/Rumos. Caso não tenha disponibilidade ou não pretenda realizar o exame de forma presencial e prefira uma solução remota acresce uma taxa de 89€ ao valor do curso.

Metodologia

About the Exam:

- Exam Prefix: 312-40 (ECC EXAM)
- Number of Questions: 125
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Test Delivery: EC-Council Exam Portal

Programa

- Module 01: Introduction to Cloud Security
- Module 02: Platform and Infrastructure Security in the Cloud
- Module 03: Application Security in the Cloud
- Module 04: Data Security in the Cloud
- Module 05: Operation Security in the Cloud
- Module 06: Penetration Testing in the Cloud
- Module 07: Incident Detection and Response in the Cloud
- Module 08: Forensics Investigation in the Cloud
- Module 09: Business Continuity and Disaster Recovery in the Cloud
- Module 10: Governance, Risk Management, and Compliance in the Cloud
- Module 11: Standards, Policies, and Legal Issues in the Cloud
- Appendix (Self-Study): Private, Hybrid, and Multi-Tenant Cloud Security