CSE – Cloud Security Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 10h

Sobre o curso

Cloud Security Essentials is a foundational course covering cloud computing and security fundamentals, data protection and encryption in the cloud and more. This course prepares you to secure identities, data, and applications within cloud providers and hybrid infrastructures. No IT/Cybersecurity experience required for this course.

Test your skills with Capstone Project and validate these newly acquired skills in proctored exams. With 6 hands-on labs and 10+ hours of premium training, the CSE provides learners with practical skills to secure cloud solutions.

Key Features:

- 6 lab practical exercises
- 10+ hours of premium self-paced video training
- 900+ pages of eCourseware
- Capstone Project
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with 1-year validity
- Get globally recognized EC-Council’s certification
- Learn about cloud adoption to cloud security with easy-to-follow modules. Enhance your value in the job market

What skills you’ll learn

- Learn the fundamentals of cloud computing and security.
- Explore identity and access management in the cloud.
- Learn about data protection and encryption in the cloud.
- Gain knowledge of network security in cloud environments.

- Dive deep into application security in cloud environments.
- Gain insights on cloud security monitoring and incident response.
- Explore cloud security risk assessment and management.
- Understand the basics of cloud compliance and governance.

Destinatários

Who Is CSE for?

- High School/College/University students
- Teams and organization
- Career starters
- Working professionals

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Training Details: Self-paced in demand lecture videos led by world-class instructors and hands-on labs.

Exam Details:

- Exam Code: 112-54
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Cloud Computing and Security Fundamentals
- Identity and Access Management (IAM) in the Cloud
- Data Protection and Encryption in the Cloud
- Network Security in Cloud
- Application Security in Cloud
- Cloud Security Monitoring and Incident Response
- Cloud Security Risk Assessment and Management
- Cloud Compliance and Governance

Cloud Computing and Security Fundamentals

- Cloud Computing Types and Service Models
- Cloud Security Challenges and Concerns
- Cloud and Security Responsibility
- Evaluating Cloud Service Providers
- Cloud Security Benefits
- Threats and Attacks in Cloud Environments
- Cloud Security Design Principles
- Cloud Security Architecture

Identity and Access Management (IAM) in the Cloud

- IAM Fundamentals
- Principal and Roles of IAM in the Cloud
- Role-based Access Control (RBAC)
- Identity Federation
- Single Sign-on (SSO) and Self-Service Password Reset (SSPR)
- Multifactor Authentication (MFA)
- Principle of Least Privilege
- IAM Auditing and Monitoring

Data Protection and Encryption in the Cloud

- Data Classification and Lifecycle
- Encryption Techniques (at Rest, in Transit)
- Customer vs. Cloud Provider Managed Keys
- Data Loss Prevention (DLP)
- Backup and Disaster Recovery Strategies

Network Security in Cloud

- Cloud Network Fundamentals
- Virtual Private Clouds (VPC)
- Network Isolation and Segmentation
- Network Access Control Lists (NACLs) and Network Security Groups (NSG)
- Remote Access and Connections
- Firewalls and Intrusion Detection

Application Security in Cloud

- Secure Software Development Lifecycle (SDLC) in the Cloud
- Web Application Firewall (WAF) in Cloud Environments
- Web Application Security and OWASP Top Ten
- Security by Design Principles for Cloud Applications
- Secure Coding Practices
- API Security and Integration Best Practices
- Serverless Security Considerations
- Container Security (Docker, Kubernetes)

Cloud Security Monitoring and Incident Response

- Cloud Logging
- Cloud Security Monitoring
- SIEM and SOAR
- Cloud-native Monitoring Solutions
- Continuous Security Monitoring Strategies
- Cloud Security Monitoring Best Practices
- Incident Response in Cloud

Cloud Security Risk Assessment and Management

- Identifying Cloud Security Risks
- Risk Assessment Frameworks for Cloud Environments
- Cloud Security Controls and Countermeasures
- Threat Modeling and Vulnerability Assessment in Cloud Environments
- Quantitative vs. Qualitative Risk Assessment Approaches
- Cloud Risk Treatment, Response, and Mitigation

Cloud Compliance and Governance

- Regulatory and Industry Compliance
- Cloud Security Standards
- Cloud Security Governance and Risk Management
- Auditing and Monitoring Cloud Resources
- Cloud Security Assessment and Penetration Testing