C|SE Cloud Security Essentials

EC-Council
Building A Culture Of Security

Cloud Security Essentials
COURSE OUTLINE

EC-Council Official Curricula

Cloud Security Essentials -v1

Course Outline

Module 01: Cloud Computing & Security Fundamentals

- Cloud Computing and Security Fundamentals
- What Is Cloud Computing?
- **Cloud Computing Types and Service Models**
  - Different Types of Cloud Deployment Models
  - Different Types of Cloud Deployment Models: Private
  - Different Types of Cloud Deployment Models: Public
  - Different Types of Cloud Deployment Models: Hybrid
  - Different Types of Cloud Service Models
  - Different Types of Cloud Service Models: Infrastructure as a Service (IaaS)
  - Different Types of Cloud Service Models: Platform as a Service (PaaS)
  - Different Types of Cloud Service Models: Software as a Service (SaaS)
- **Cloud Security Challenges and Concerns**
  - Cloud Security Challenges and Concerns
- **Cloud and Security Responsibilities**
  - Cloud Shared Responsibilities
  - Shared Responsibility Model for Cloud and Security
- **Evaluating Cloud Service Providers**
  - Cloud Service Providers (CSP)
  - Comparing The Top 3 Cloud Service Providers (CSPs)
  - Comparing The Top 3 Cloud Service Providers (CSPs): Microsoft
  - Comparing The Top 3 Cloud Service Providers (CSPs): AWS
  - Comparing The Top 3 Cloud Service Providers (CSPs): GCP
- **Cloud Security Benefits**
  - Cloud Characteristics

- Cloud Security Benefits

- **Threats and Attacks in Cloud Environments**
  - Threats And Attacks in Cloud Environments
  - OWASP Cloud-Native Application Security Top 10
  - Phishing
  - Spear Phishing
  - Denial-Of-Service Attack
  - Brute Force Attacks
  - Web Attacks
  - SQL Attacks
- **Cloud Security Design Principles**
  - C-I-A Triad
  - Defense In Depth
  - Zero Trust Methodology
  - Google Cloud Adoption Framework
- **Cloud Security Architecture**
  - Cloud Transformation and Security Architecture
  - Secure Landing Zones
  - AWS Architecture Example
  - GCP Architecture Example
  - AZURE Architecture Example
  - Google Cloud Adoption Framework

Module 02: Identity And Access Management (IAM) in the Cloud

- **IAM Fundamentals**
  - IAM Fundamentals
  - Key IAM Terms
  - Defining IAM
  - Legacy vs. Modern IAM
  - Active Directory Authentication
  - Cloud Identity Provider
  - Cloud Identity Governance
- **Principal and Roles of IAM in the Cloud**
  - Cloud Identity Governance
  - Role Permissions
- **Role-based Access Control (RBAC)**
  - Role-based Access Control (RBAC)

- **Identity Federation**
  - Identity Federation
  - Hybrid Identity Federation
  - Multicloud Identity Federation
  - Cloud and External Provider Federation
- **Single Sign-on (SSO) and Self-Service Password Reset (SSPR)**
  - Single Sign-on (SSO)
  - Self-Service Password Reset (SSPR)
- **Multifactor Authentication (MFA)**
  - Multifactor Authentication (MFA)
- **Principle of Least Privilege**
  - Principle of Least Privilege
  - Conditional and Behavior Based Access
- **IAM Auditing and Monitoring**
  - IAM Auditing and Monitoring

Module 03: Data Protection and Encryption in the Cloud

- **Data Classification and Lifecycle**
  - Governing And Securing Your Data
  - Data Classification
  - Protect Your Data
  - Project Overview
  - Data Retention
  - Governing And Securing Your Data
- **Encryption Techniques (at Rest, in Transit)**
  - Encryption Types
  - Governing And Securing Your Data
  - Encryption In Transit
- **Customer vs. Cloud Provider Managed Keys**
  - Customer Vs. Cloud Provider Managed Keys
  - Key Management in the Cloud
  - Azure Key Vault
  - AWS Key Management Service
  - Google Cloud Platform Encryption
- **Data Loss Prevention (DLP)**
  - Data Loss Prevention
  - Cloud Provider Data Loss Prevention (DLP) Solutions

- **Backup and Disaster Recovery Strategies**
  - Backup Vs. Replication
  - Cloud-Based Site Recovery
  - Cloud Backup

Module 04: Network Security in Cloud

- **Cloud Network Fundamentals**
  - Cloud Networks
- **Virtual Private Clouds (VPC)**
  - AWS VPC Architecture
  - Azure Virtual Network (VNET)
- **Network Isolation and Segmentation**
  - Network Segmentation
  - AWS Elastic Load Balancers
  - Azure Front Door and Application Gateway
  - DDoS Protection
- **Network Access Control Lists (NACLs) and Network Security Groups (NSG)**
  - AWS NACL and Security Groups
  - Azure Network Security Groups (NSG)
- **Remote Access and Connections**
  - VPC Endpoint Connections
  - AWS Remote Connections with Transit Gateway
  - Azure Private Links
  - Remote Management – Azure Bastion
  - Just in Time VM Access
  - AWS NAT Instances Vs. NAT Gateways
  - NAT Instance Vs. Bastion host
- **Firewalls and Intrusion Detection**
  - Azure Firewall
  - Web Application Firewall
  - AWS Web Application Firewall (WAF)
  - Intrusion Detection Vs. Intrusion Prevention

Module 05: Application Security in Cloud

- **Secure Software Development Lifecycle (SDLC) in the Cloud**
  - Secure Software Design
  - Cloud Security Controls within Security Objective

- Secure Software Development Lifecycle

- **Web Application Firewall (WAF) in Cloud Environments**
  - Why use a WAF?
  - Web Application Firewall in Azure
  - AWS Web Application Firewall (WAF)
- **Web Application Security and OWASP Top Ten**
  - Common Attacks
  - Ransomware Attack
- **Security by Design Principles for Cloud Applications**
  - Secure Application Design
  - Traceability of Data
  - Data Integrity
  - Key Secure Software Design Concepts
  - DevSecOps
- **Secure Coding Practices**
  - Secure Code Testing
  - Runtime Application Self-Protection (RASP)
- **API Security and Integration Best Practices**
  - API Security Design and Development
  - AWS Config
  - Secure Azure API Management
- **Serverless Security Considerations**
  - Serverless Security Practices
  - Azure Functions Security
  - Web Application Firewall
- **Container Security (Docker, Kubernetes)**
  - AWS Config
  - Container Security Practices

Module 06: Cloud Security Monitoring and Incident Response

- **Cloud Logging**
  - Importance of Logging
  - Cloud Logging
- **Cloud Security Monitoring**
  - Cloud Native Tools
  - Azure Monitor
  - Azure Network Watcher
  - Log Analytics

- Azure Arc
- AWS CloudTrail
- AWS CloudWatch

- **SIEM and SOAR**
  - Information and Event Management
  - SIEM AND SOAR
- **Cloud-native Monitoring Solutions**
  - Security Posture Management
  - Microsoft Defender for Cloud - CSPM
  - Amazon Security Hub
- **Continuous Cloud Security Monitoring**
  - Cloud Native Application Protection Platform (CNAPP)
  - Microsoft Defender for Cloud - CNAPP
  - CNAPP capabilities within AWS using CloudGuard
  - Google Cloud Armor CNAPP
- **Incident Response and Investigation in the Cloud**
  - Timeline of A Breach
  - Incident Response

Module 07: Cloud Security Risk Assessment and Management

- **Identifying Cloud Security Risks**
  - Cloud Risk Assessment Checklist
  - Common Cloud Security Risks
  - Top Cloud Vulnerabilities
  - Risk Categories
- **Risk Assessment Frameworks for Cloud Environments**
  - Risk Management Tiers
  - Risk Management Strategy
  - NIST Risk Management Framework SP 800-37 REV. 2
- **Cloud Security Controls and Countermeasures**
  - Defense In Depth
  - Security Controls and Countermeasures
  - Business Continuity Plans
  - Disaster Recovery Plan
  - BCP and DRP Working Together
- **Threat Modeling and Vulnerability Assessment in Cloud Environments**
  - Cloud Threat Modeling
  - Cloud Threat Modeling Resources

- Vulnerability Assessments
- Vulnerability Scanning

- **Quantitative vs. Qualitative Risk Assessment Approaches**
  - Risk Analysis
  - Qualitative Risk Analysis
  - Qualitative Risk Analysis
  - Risk Analysis Decision Matrix
- **Cloud Risk Treatment, Response, and Mitigation**
  - Residual Risk
  - Risk Response
  - Responses To Risk

Module 08: Cloud Compliance and Governance

- **Regulatory and Industry Compliance**
  - Regulatory Compliance
  - General Data Protection Regulation (GDPR)
  - Federal Information Security Management Act (FISMA)
  - Family Educational Rights and Privacy Act (FERPA)
  - International Standards Organization (ISO)
  - National Institute of Standards & Technology (NIST)
  - NIST SP 800-53
  - FedRAMP
  - Industry Compliance Standards
  - PCI-DSS
  - 2023 UPDATES to PCI-DSS
  - Sarbanes-Oxley Act (SOX)
  - GLBA
  - HIPAA
  - HIPAA Security Rule
  - HITRUST Common Security Framework
  - HITRUST Certification
- **Cloud Security Standards**
  - Cloud Security Standards
  - NIST Cybersecurity Framework
  - ISO 27001
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)

- CSA Cloud Control Matrix
- CSA Cloud Control Matrix List of Controls

- **Cloud Security Governance and Risk Management**
  - Keys To Maintaining Compliance
  - Cloud Security Governance
  - Cloud Security Assessments and Auditing
  - Cloud Security Assessments Methodology
  - Cloud Security Assessments Challenges
  - Cloud Monitoring and Management
  - Risk Management Process
  - Responses To Risk
- **Auditing and Monitoring Cloud Resources**
  - Cloud-Native Auditing
  - Azure Policy
  - Microsoft Defender For Cloud
  - AWS Config Manager
  - AWS Inspector
  - Google Cloud Compliance Reports Manager
- **Cloud Security Assessment and Penetration Testing**
  - Cloud Security Assessments
  - Cloud Security Assessment
  - Cloud Security Assessment
  - Ethical Penetration Testing
  - Cloud Penetration Testing and Limitations