The rapidly evolving information security landscape now requires professionals to stay up to date on the latest security technologies, threats and remediation strategies. CAST was created to address the need for quality advanced technical training for information security professionals who aspire to acquire the skill sets required for their job functions. CAST courses are advanced and highly technical training programs co-developed by EC-Council and well-respected industry practitioners or subject matter experts. CAST aims to provide specialized training programs that will cover key information security domains, at an advanced level.
Most businesses around the world, small and large, use multiple cloud services to handle business-critical data. Though cloud services offer improved efficiency, reduced costs, greater accessibility and flexibility, they also increase security risk. Cloud leaders focus on measures to reduce data breaches, maintain confidentiality, and preserve integrity, authenticity and completeness. Other areas of concern are risk factors associated with virtual machines, vulnerabilities from shared resources, and issues with encryption.

Recent hacking attacks on Dropbox, Google's DNS, LinkedIn, etc. are only indications of larger threats to cloud services and data security. According to McAfee® Labs 2014 Threats Predictions report, deployment of cloud-based corporate applications will create new attack surfaces that will be exploited by cybercriminals.

The Designing and Implementing Cloud Security course provides comprehensive knowledge of cloud services, their characteristics, benefits, applications, and service models. The course will help professionals understand the risks and threats associated with cloud service adoption and migrating business-critical data to third party systems.

The program covers planning, designing, and implementing cloud security controls. It delves into various cloud standards, countermeasures, and best practices to secure information in the cloud. The program also emphasizes the business aspects of cloud security such as cloud uptime, uptime guarantee, availability, fault tolerance, fail-over policy, and how cloud security strengthens the business case for cloud adoption.
Designing and Implementing Cloud Security

The Program Addresses Critical Cloud Governance, Risk Management, and Compliance (GRC) Issues

01 Encryption
02 Key Management
03 Identity and Access Management
04 Privacy Breach
05 Cloud Forensics
06 Penetration Testing

The Designing and Implementing Cloud Security course prepares IT and business leaders to address the risks and challenges of cloud adoption.
After completing this course, students will learn:

01. Fundamentals of cloud computing, cloud services, its characteristics, benefits, and applications
02. Cloud computing service models, deployment models and security considerations of cloud computing
03. Secure cloud computing environment design
04. Data center, online storage options, cloud based server capacity, and cloud server virtualization
05. Cloud computing standards
| 06 | Cloud uptime, optimizing cloud performance, availability and its characteristics |
| 07 | Cloud fault tolerance, load balancing, and cloud failover policies |
| 08 | Best practices of virtualization and cloud implementation |
| 09 | Cloud security, cloud security control layers, encryption and key management, identity access management, federated identity management, and IAM standards for consumers |
| 10 | Cloud configuration management, patching modes, standardized policy creation, and cloud-based patch management tools |
| 11 | Cloud computing risk assessment and cloud penetration testing |
| 12 | Intrusion detection systems (IDS) in a cloud environment |
| 13 | Types of attacks on a cloud environment and techniques to overcome attacks |
| 14 | Legal issues such as cloud computing contracts, vendor transitioning, auditing cloud data, maintaining privacy and confidentiality, geographic jurisdiction, limitations on vendor liability, and taxation challenges |
| 15 | Compliance to established industry standards, acts, and laws including PCI-DSS, HIPAA, Sarbanes-Oxley, and Data Protection Act |
Who Should Attend

- IT Security Managers
- Cloud Security Professionals
- Entrepreneurs
- Database and Web Developers
- Security Auditors and Compliance Managers
- Network and System Administrator

Duration

3 days (9:00 – 5:00)
Course Outline

Module 01: Fundamentals of Cloud Computing

- Cloud Computing
- Cloud Computing Characteristics
- Benefits of Cloud Computing
- Economics of Cloud Computing
- Application of Cloud Computing in Various Domains
- Cloud Computing for Enterprises
- Linux Security Countermeasures
- Cloud Computing Service Models
- Cloud Deployment Models
- Private Cloud Computing
- Public Cloud Computing
- Hybrid Cloud Computing

- Community Cloud Computing
- Cloud Computing Service Model Applications
- Challenges in Cloud Computing Adoption
- Major Barriers to Cloud Computing Adoption
- 7 Steps for Migrating Services to Cloud
- What Should Not be Moved to the Cloud
- Cloud Computing Security Risks
- Cloud Computing Attacks
- Cloud Computing Security Considerations
- Cloud Security Best Practices
- Case Study
Module 02: Designing a Secure Cloud Computing Environment

- Layers of Cloud Computing
- Single and Multi-Tenancy Environments
- Cloud SLA
- Service Oriented Architecture
- Cloud Deployment Requirements
- Cloud Networking
- Monitoring Performance
- Communication Requirements for Cloud
- Cloud Security
- Physical vs. Virtual Security
- Cloud Application Security Best Practices
- Prerequisites for Building your Cloud Infrastructure
- Cloud Computing Reference Architecture, Models and Framework
- Cloud Cube Model
- Types of Data Centers
- Data Center Design Standards
- Data Center and Cloud
- Cloud Computing and Cloud Storage

- Cloud Storage Networks
- Cloud Computing Providers
- Google’s Cloud
- Build, Debug and Deploy Apps for Google App Engine using eXo Cloud IDE
- Open Source Data Center and Cloud Software
- Pros and Cons in Deploying Open-Source Cloud Systems
- Cloud-based Server Capacity
- Cloud Server Capacity Providers
- Do’s and Don’ts of Cloud-based Server Capacity
- Cloud Server Virtualization
- Cloud Capacity Planning Tool: Server File System
- Analytics Utility: CopperEgg
- Xeround Cloud Database for MySQL Applications
Module 03: Cloud Computing Standards

Why Cloud Environment Need Standards?

Benefits of Standardized Policies

Cloud Ecosystem and Standards

Role of Cloud Standard Organizations

Standards Development Organizations in Cloud Computing
Module 04: Cloud Uptime and Availability

- Terminology
- Cloud Outage/Failure and their Impacts
- Importance of ‘Uptime Guarantee’
- Recommendations for Maximizing Uptime
- Pingdom
- Cloud Uptime Monitoring Tools
- Cloud Availability
- Recommendations for Cloud Providers to Improve Availability
- Recommendations for Cloud Users to Improve Availability

- Data Backup on Cloud
- Cloud Backup and Disaster Recovery Benefits
- High Availability Definition
- Fault Tolerance
- Fault Tolerance Techniques
- HAProxy - The Reliable, High Performance TCP/HTTP Load Balancer
- Cloud Failover Policy
- SaaS-Specific Rider
- PaaS-Specific Rider
- IaaS-Specific Rider
- Geminare’s Cloud Recovery/Auto Failover
- Load Balancing

- Lessons to be Learnt from Cloud Outages
- Rackspace Cloud Load Balancer Control Panel
- Load Balancing Solutions
- Best Practices for Optimal Cloud Performance
Virtualization Terminologies

Why we need Virtualization for Cloud?

Introduction to Virtualization

Virtualization Vendors

Importance of Virtualization

Datacenter & Cloud Infrastructure Product: vSphere

Characteristics of Virtualization

Virtualization Vendors

Virtualization Techniques

Virtualization Security Best Practices for Administrators

Type 1 and Type 2 Hypervisors

Best Practices for VM Security

CAST & PVODJM
Module 05: Virtualization on Cloud
CAST & PVODJM

EC-Council
## Module 06: Cloud Security

- What is Cloud Security?
- Top Ten Threats to Cloud Security
- Data Breach
- Data Loss
- Account Hijacking
- Insecure Interfaces and APIs
- Denial-of-Service (DoS)
- Malicious Insiders
- Abuse of Cloud Services
- Password Cracking Services on Cloud
- Insufficient Due Diligence
- Shared Technology Issues
- Unknown Risk Profile
- Cloud Sprawl
- Cloud Security Controls
- Cloud Security Control Layers
- Placement of Security Controls in the Cloud
- Cloud Security is the Responsibility of both Cloud Provider and Consumer
- Encryption and Key Management
- Tips to Protect Encryption Keys
- Enhancing Encryption Strength: Hardware/Software Protection
- Identity and Access Management (IAM)
- Securing Identity Provisioning
- Securing Authentication in Saas and Paas Environments
- Securing Authentication in Saas and IDaaS Environments
- Federated Identity Management
- Securing Federated Identity Management
- Securing Access in Clouds
- Using Security Assertion Markup Language (SAML) for Federated Single Sign-on
- Using Service Provisioning Markup Language (SPML) for IAM
- Using eXensible Access Control Markup Language (XACML) for IAM
- Using Open Authentication (OAuth) for IAM
- IAM Standards for Consumers
- CloudPassage
- Cloud Security Vendors
- Best Practices for Securing Cloud
Module 07: Cloud Configuration and Patch Management

- Cloud Configuration Management
- Cloud Configuration Management Approaches
- VMware vCenter Configuration Manager
- NephoScale’s Configuration Management
- Configuration Management Systems
- Patch Management Challenges in Cloud
- Vulnerable Areas that need Patch in Cloud
- Patch Management Process Workflow
- Patch Management Process Flow Overview
- Patch Management Process
- Major Challenges to the Patch Management Flow
- Key Considerations for Patch Management in Cloud
- Creating Standardized Patch Management Policies
- Cloud-based Patch Management tools
- Checklist for Selecting a Cloud Patch Service Provider
Module 08: Penetration Testing and Risk Assessment

- Cloud Computing Risk Assessment
- Cloud Computing Risk Categories
- Risk Assessment Metrics
- What is Cloud Pen Testing?
- Why Penetration Testing?
- Penetration Test vs. Security Assessment
- Phases of Penetration Testing
- Key Considerations for Pen Testing in the Cloud
- Scope of Cloud Pen Testing
- Cloud Penetration Testing Steps
- Recommendations for Cloud Testing
- Introduction to Virtualization
- Prerequisites to Virtual Machine Pen Testing
- Virtual Environment Pen Testing
- Virtual Machine Penetration Testing Steps
- Vulnerability Assessment Tool
- Configuration Management Tools
- Virtualization Assessment Toolkit
- Virtualization Best Practices
Module 09: Cloud Computing Legal Issues

- Key Legal Issues
- Cloud Computing Contracts
- General Terms used in Cloud Contracts
- Non Negotiable Contracts
- Issues with Sub Contracts
- Business Continuity Issues
- Interoperability Issues
- Getting through SLAs
- Vendor Transitioning
- Tracking and Auditing Cloud Data
- Privacy and Confidentiality
- Geographic Jurisdiction
- Limitations on Vendor Liability
- Ending the Arrangement
- Compliance and Audit
- Compliance Contract Challenges
- Recommendations for Compliance and Audit
- Taxation Challenges
- Cloud Computing Legal Checklist
- Checklist for Invalidating Legal Issues in Cloud Provider Selection
- 9 Questions to Ask Before Signing a Cloud Computing Contract
- 9 Best Practices for Cloud Computing Contracts
- Cloud Computing Acts
Module 10: Using iPhones, Tablets and other devices to Access Cloud

- Mobile Cloud Computing (MCC)
- Mobile Cloud Computing Applications
- Operating Systems for Smartphones
- Mobile Web Browsers
- Cloud Apps on Smartphones
- Benefits of Mobile Access to Cloud
- Limitations of Mobile Access to Cloud
- Mobile Virtualization Platform (MVP)
- Mobile E-commerce Security Checkpoints
- Virtual Terminal
- Working of a Virtual Terminal

- Virtual Terminal Security Benefits
- Mobile Cloud Collaboration Applications
- iPhone apps for Business Collaboration
- Android apps for Collaboration
- Mobile Spy
- Stolen Mobile Tracking Software
- Threats of Mobile Malware
- Mobile Cloud Threats and Countermeasures
- Mobile Client Security Software
- How to Set a Passcode on Lock Screen of iPhone 5
- Secured Mobile Cloud Access
- Mobile Device Security Guidelines for Administrator
- General Guidelines for Mobile Platform Security
- Best Practices for Secured Mobile Cloud Access
Master Trainer:

Haja Mohideen
VP- TECHNOLOGY, EC- COUNCIL

Mr. Haja Mohideen is the VP- Technology and Co-Founder of EC-Council. He manages the certifications and training programs for EC-Council, and leads the product development team. He is known worldwide as the creator of the popular EC-Council certification programs Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified System Analyst / Licensed Penetration Tester (ECSA/LPT) and EC-Council Certified Secure Programmer (ECSP), among others.

Haja has 17 years of experience specializing in the development, support and project management of PC software and hardware. He has trained various Fortune 500 companies as well as US government agencies. He is also the Master Trainer for EC-Council courses, and his training is often sought after globally. He has led training in many countries including Greece, India, USA, Indonesia, Singapore, England, Mexico, amongst others. Haja is also one of few who are qualified to conduct train the trainer sessions for EC-Council courses.

Haja holds a Masters Degree in Software Engineering and has numerous industry-wide IT certifications from Microsoft, IBM, Cisco, Motorola, 3COM, Adobe, Intel and many others. He carries over 90 vendor certifications.