Practitioner Certificate in Cloud Security

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

https://bilginc.com/tr/egitim/practitioner-certificate-in-cloud-security-681-egitimi/

Overview

This five day Certified Cloud Security Practitioner course is focused on Cloud Security, encompassing Cloud Security Architecture, DevSecOps, Data and Assurance aspects, Governance, Cloud Security Operations and Web Application Security.

The course spans cloud security principles, patterns and architectural frameworks, data protection and compliance for cloud based applications, data and infrastructure, and the design, development and implementation of cloud security architectures.

We will review the wide range of technical security controls available using Cloud Service Provider and partner technologies, automation and DevSecOps, assurance, audit and security testing of cloud based services. Containers and serverless architectures will be introduced and their security implications reviewed. Agile DevOps methodologies will be covered and the use of a Continuous Integration Pipeline for security improvements, validation and testing.

The course is delivered through presentations, discussions, practical demonstrations and 'hands-on' labs. You will gain practical hands-on experience of implementing and using cloud technologies and technical security controls in labs based on services from leading cloud service providers AWS and Microsoft, and consolidate learning in group workshops to develop cloud security architectures, based on realistic scenarios.

Target Audience

This course is aimed at technical and security specialists looking to develop and operate secure applications and systems using an agile DevOps methodology with fully automated deployments to cloud environments.

IISP Skills Alignment

This course is aligned to the following Institute of Information Security Professionals (IISP) Skills. More details on the IISP skills framework can be found here.

- A1, A2, A6, A7, B1, B2, C1, C2, D1, D2, E1, E2, G1

Continuous Professional Development (CPD)

CPD points can be claimed for GCT accredited courses at the rate of 1 point per hour of training for GCHQ accredited courses (up to a maximum of 15 points).

Prerequisites

There are no pre-requisites. However, we recommend that all delegates have an understanding of the general technologies, for example Operating Systems and Networking and Security principles. Experience of using cloud services and security technologies is helpful but not essential.

For those delegates looking for some pre-course general cloud security background, guidance and organisational compliance, the NCSC cloud security collection is probably the single best resource.

What You Will Learn

Delegates will learn about the following topics:

- Cloud Concepts
- Virtualisation
- Cloud Security Frameworks, Principles, Patterns and Certifications
- AWS Security Technologies
- Microsoft Azure and Office 365
- Google Cloud Platform and G Suite
- Assurance
- Data Protection and Compliance
- Containers

- Web Application Security
- Cloud Identity Services
- Serverless
- Cloud Security as a Service
- Automation
- Continuous Integration Pipeline
- DevSecOps

Outline

DAY ONE

Introduction

- Introductions
- Objectives of course
- Agenda

Cloud Concepts

- What is Cloud Computing?
- Why is everyone moving to the Cloud?
- Cloud computing model
- Infrastructure, Platform and Software as a Service
- Boundaries and responsibilities
- Cloud Service Providers – Gartner Magic Quadrant(s)
- Cloud reference architectures

Virtualisation

- Overview of different virtualisation technologies and types covering storage, networks and systems.

Cloud Security Frameworks, Principles, Patterns and Certifications

- Security Principles
- Separation and layers as security controls
- Cloud Security Alliance (CSA) Cloud Control Matrix
- GOV.UK Cabinet Office and NCSC Cloud Security Principles
- Security Architecture Frameworks
- Security Architecture Patterns
- Cloud Security Architecture Patterns
- Trusted Cloud Initiative Reference Architecture
- Cloud Security Certifications

AWS Security Technologies

- EC2 (Elastic Compute Cloud) and VPC (Virtual Private Cloud) fundamentals
- Availability zones and regions
- Internet Gateway, Elastic IPs, NAT Gateway, DirectConnect
- Security Implications of Elastic Load Balancing (ELB) and auto-scaling
- Security Groups, Flow Logs, S3, ACLs and subnet routing
- AWS Config, CloudTrail, CloudWatch, Trusted Advisor
- IPSec VPN options: AWS VPNs, third party solutions
- AWS CloudFront, Web Application Firewall and Certificate Manager
- Vulnerability management using AWS Inspector
- AWS Key Management Service (KMS) and CloudHSM
- AWS Identity and Access Management (IAM)
- Labs providing practical experience of implementing and using AWS security technologies

Quiz

- End of day knowledge check – exam style questions

DAY TWO

Microsoft Azure and Office 365

- Azure platform security architecture
- Azure Virtual Networks
- Azure network security best practices
- Azure data security and encryption best practices
- Azure Active Directory
- Federated identity and Single Sign On
- Azure Multi-factor authentication
- Azure Key Vault
- Azure Virtual Machine encryption
- Microsoft Antimalware for Azure Cloud Services and Virtual Machines
- Azure Security Center
- Office 365 Service Architectures
- Office 365 security across physical, logical and data layers
- Office 365 email encryption options
- Exchange Online Protection
- GOV.UK Microsoft Office Security Guidance
- Labs providing practical experience of implementing and using Microsoft Azure security technologies

Google Apps for Work

- Google Apps for Work applications and architectures
- Integration with corporate directories
- Single sign-on to enforce use of corporate devices and threat prevention
- GOV.UK Google Apps for Work Security Guidance
- Google Admin Console
- Google Authenticator
- Organisational Units
- Administrative roles
- Data privacy opt-in

Assurance

- Centre for Internet Security (CIS) Foundation Benchmarks
- Penetration tests of cloud environments
- External audit and configuration review

Data Protection and Compliance

- Personally Identifiable Information (PII) and Personal Data
- UK Data Protection Act and Information Commissioner’s Office (ICO)
- European Union (EU) Data Protection Directive
- EU General Data Protection Regulation (GDPR)
- Cyber Essentials Plus
- Cloud Security Alliance STAR
- PCI DSS
- AICPA SOC3 (formerly SAS70)
- ISO 27001

Quiz

- End of day knowledge check – exam style questions

DAY THREE

Containers

- Concept of containers
- Docker
- Why development teams are moving to containers
- Security issues of containers
- Container security good practice
- CIS Benchmark for Docker and Docker Bench tool
- Orchestration – Kubernetes
- Security features of Kubernetes
- Orchestration – Docker Swarm
- Cloud Service Provider container platforms (AWS, Azure, Google)
- Container security solutions (e.g. Twistlock, NeuVector, AquaSecurity)

- Labs providing hands-on experience of Docker containers and potential security issues

Web Application Security

- OWASP Top 10
- Threat Modelling
- Secure Software Development Lifecycle

Cloud Identity Services

- SAML
- oAuth, oAuth 2.0 and OpenID Connect
- Cloud Identity Providers

Quiz

- End of day knowledge check – exam style questions

DAY FOUR

Serverless

- Concept of ‘serverless’
- Pros and Cons
- AWS Lambda
- Step functions
- Dynamo DB
- SQS, SWS, S3
- Serverless application architecture
- Security implications
- Environment Variable encryption
- Azure Cloud Functions
- Google Cloud Functions
- Labs providing hands-on experience of Serverless architectures

Cloud Security as a Service

- Cloud Security Services
- Cloud analytics, e.g. Splunk Cloud
- Cloud security operations management, e.g. AlertLogic

Quiz

- End of day knowledge check – exam style questions

Cloud Security Workshop

- Scenario requirement
- Develop security architecture in groups
- Present back to wider group, review and discuss

DAY FIVE

Automation

- Cloud service provider automation tools
- Terraform by Hashicorp
- Hardened build images
- Vault by Hashicorp
- Patching and update strategies
- DevSecOps

Continuous Integration Pipeline

- Continuous Integration Pipeline
- Automated environment testing
- Jenkins
- Security issues

DevSecOps Lab

- Hands-on experience of coding security improvements and automated deployments

Quiz

- End of section quiz – exam style questions

Exam Information - For Classroom based events:

Candidates will receive individual emails to access their AMPG GCT candidate portal, typically available two weeks post exam. If you experience any issues, please contact the APMG GCT technical help desk on 01494 4520450.

Duration	70 minutes
Questions	70, multiple choice (4 multiple choice answers only 1 of which is correct)
Pass Mark	50%

Exam Information - For Attend from Anywhere events:

The (Attend from Anywhere) exam is a Proctor-U APMG exam for the Practitioner Certificate in Cloud Security, which will be taken by delegates in their own time after the course. Delegates will receive individual emails to access their AMPG GCT candidate portal, typically available two weeks post exam.

If you experience any issues, please contact the APMG GCT technical help desk on 01494 4520450.