Practitioner Certificate in Cloud Security Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This NCSC Assured hands-on (25+ labs) five-day vendor agnostic Practitioner Certificate in Cloud Security course is focused on Cloud Security, encompassing Cloud Security Architecture, Cloud Security Testing, Identity & Access Management, DevSecOps, Cloud Data Security, Cloud Assurance, Governance, Cloud Security Operations and Web Application Security, and Zero Trust in the Cloud and Cloud Supply chain.

The course spans cloud security principles, patterns and architectural frameworks, data protection and compliance for the three major cloud providers, cloud-based applications, data and infrastructure, and the design, development and implementation of cloud security architectures. This course that will expose you to a variety of cloud security and assurance aspects across the 3 big cloud computing platforms - AWS, Azure and GCP. It has been specifically blended with 25+ of the most up to date cloud security labs, from our QA Group platform. Learners will have 1 month access to the QA Group platform as part of the course.

We will review the wide range of technical security controls available using Cloud Service Provider and partner technologies, automation and DevSecOps, Kubernetes auditing, assurance, audit, and security testing of cloud-based services. Zero Trust in the cloud and cloud supply chain. 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.

Continuous Professional Development (CPD)

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

Prerequisites

There are no pre-requisites.

Target Audience

This hands-on vendor agnostic course is aimed at technical and security specialists looking to develop and operate secure applications and systems in the cloud.

Practitioner Certificate in Cloud Security Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Delegates will learn about the following topics:

- Cloud Concepts
- Cloud Virtualisation
- Cloud Network Security Fundamentals
- AWS Core Services
- AWS Security Technologies
- Azure Core Services
- Azure Security and Microsoft 365
- Google Cloud Core Services
- Google Cloud Security
- Cloud Security Frameworks, Principles, Patterns and Certifications
- Container Security
- Cloud Native Computing
- Serverless Security
- Cloud Assurance
- Web Application Security
- Cloud Identity Services
- Cloud Security Services
- Automation and Continuous Integration
- DevSecOps
- Zero Trust Architecture
- Zero Trust Governance

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.

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

Network Security Fundamentals

- IPv4 and IPv6
- DNS
- Firewalls
- Network Address Translation
- IPSec VPN

AWS Core Services

- EC2 (Elastic Compute Cloud) and VPC (Virtual Private Cloud) fundamentals
- Availability zones and regions
- Internet Gateway, Elastic IPs, NAT Gateway
- VPN Gateway, DirectConnect
- VPC Peering, AWS Transit Gateway
- Security Groups, Flow Logs, NACLs and subnet routing
- Route53
- Amazon S3

Related Labs

- *AWS - Introduction to Virtual Private Cloud (VPC)*
- *AWS - Create Your First Amazon S3 Bucket*
- *AWS - Create Your First Amazon EC2 Instance (Windows)*
- *AWS - Create Your First Amazon EC2 Instance (Linux)*

Knowledge Check – Quiz

- End of module knowledge check – exam style questions

Day Two

AWS Security Technologies

- AWS Identity and Access Management (IAM)
- AWS Organizations and SSO
- AWS CloudTrail, CloudWatch, Config, Trusted Advisor
- AWS CloudFront and Shield
- AWS WAF and Firewall Manager
- AWS Certificate Manager
- AWS Key Management Service (KMS) and CloudHSM
- AWS Secrets Manager
- AWS Inspector, Macie and Guard Duty
- AWS Artifact and Audit Manager
- AWS Security Hub
- Amazon Detective
- AWS PrivateLink and VPC Endpoints
- AWS EC2 Nitro

Azure Core Services

- Azure regions and availability zones
- Azure Active Directory
- Azure AD Connect

- Azure role-based access control
- Azure Virtual Networks
- Azure Network Security Groups
- Application Security Groups
- Remote Access and VPN
- Load Balancing
- Azure Front Door
- Azure network security best practices

Azure Security Services

- Azure Key Vault
- Azure Firewall
- Azure Virtual Machine encryption
- Microsoft Antimalware for Azure Cloud Services and Virtual Machines
- Azure Policy
- Azure Security Center
- Azure Monitor, Log Analytics and Alerts
- Azure Sentinel
- Enterprise Azure architectures

Microsoft 365 and Azure AD security

- Microsoft 365 services
- Azure AD and Microsoft 365
- Microsoft 365 security
- Microsoft Defender
- Microsoft 365 data protection and governance
- Azure AD Conditional Access and MFA
- Azure AD Password Protection
- Azure AD Identity Protection
- Azure AD Privileged Identity Management

Google Cloud core services and Google Workspace

- Google Cloud Platform services
- Compute
- Networking
- Storage and databases
- Big Data
- GCP example architecture
- Google Workspace
- Google Workspace integration with corporate directory
- Google Cloud Fundamentals: Getting Started with GKE

Related Labs

- *AWS - Detecting Malicious Web Requests With AWS Web Application Firewall*
- *AWS - Encrypting S3 Objects Using SSE-KMS*
- *Azure - Secure Your Cloud with Microsoft Defender for Cloud*
- *Azure - Using Conditional Access Policies to Enable Microsoft Entra ID Multi-Factor Authentication*
- *Azure - Managing Access in Azure Using Privileged Identity Management*
- *Azure - Using Conditional Access Policies to Enable Azure AD Multi-Factor Authentication*

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- *Azure - Managing Access in Azure Using Privileged Identity Management*
- *GCP - Create a Network Infrastructure with Google Virtual Private Cloud*
- *GCP - Inspecting and De-Identifying Data With Google Cloud Data Loss Prevention*

Knowledge Check – Quiz

- End of module knowledge check – exam style questions

Day Three

Google Cloud Security

- Identity and Access Management
- Network Security
- VPC Service Controls
- Cloud Armor
- IAP Proxy and BeyondCorp
- Confidential and shielded VMs
- Keys and Encryption
- Certificate Services
- Secret Manager
- Logging
- Organization policy constraints
- Data Loss Prevention API
- Web Security Scanner
- Container Registry Vulnerability Scanner
- Cloud Security Command Center
- Forseti

Cloud Security Frameworks, Principles and Patterns

- 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

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
- ISO 27001

Container Security

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 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 (Twistlock, AquaSecurity)

Cloud Native Computing

- Cloud Native Computing Foundation
- 12 Factors of a cloud-native app
- Cloud Native platform concepts
- Cloud Foundry
- Cloud Foundry security best practices

Related Labs

- *GCP - Inspecting and De-Identifying Data With Google Cloud Data Loss Prevention*
- *Containers - Scanning Container Images for Known Vulnerabilities*
- *AWS - Associating AWS IAM Roles with Amazon EKS Service Accounts*

Knowledge Check – Quiz

- End of module 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
- Serverless Framework

Assurance

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

Web Application Security

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- OWASP Top 10
- Secure Software Development Lifecycle

Cloud Identity Services

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

Related Labs

- *AWS - Introduction to AWS Lambda*
- *AWS - Creating Scheduled Tasks with AWS Lambda*
- *AWS - Detecting EC2 Threats with Amazon GuardDuty*
- *Kubernetes Cluster Auditing (Optional)*
- *Continuously Detecting Vulnerabilities With Amazon Inspector (Optional)*
- *OWASP - Multiple Labs*

Knowledge Check – Quiz

- End of module knowledge check – exam style questions

Day Five

Cloud Security as a Service

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

Automation, DevSecOps and Continuous Integration

- Cloud service provider automation tools
- Terraform by Hashicorp
- Hardened build images
- Vault by Hashicorp
- Patching and update strategies
- DevSecOps
- Continuous Integration Pipeline
- Automated environment testing
- Jenkins
- Security issues

Related Labs

- *AWS - Deploying Wordpress using AWS CloudFormation*
- *AWS - Static Code Analysis Within CI/CD Pipelines*

Zero Trust Architecture

- Need for Zero Trust
- Zero Trust Definition & Use case
- Zero Trust Tenets, Design Principles, Pillars
- Zero Trust Architecture - Conceptual View

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Zero Trust Benefits (Technical & Business)
- CISA High-Level Zero Trust Maturity Model
- Zero Trust - Requirement in Regulatory Frameworks

Knowledge Check – Quiz

- End of module knowledge check – exam style questions

Exams and Assessments

This course includes a formal exam, taken after the course using an exam voucher code via the APMG proctor platform.

- Format: multiple choice — 50 questions, each with four options and one correct answer

- Duration: 60 minutes

- Pass mark: 50%

Successful candidates earn the Practitioner Certificate in Cloud Security. If you experience any issues accessing the exam, contact the APMG technical help desk on 01494 452045.

Attendees are recommended to bring a smartphone or tablet upon which they can install apps: several labs use Multi-Factor Authentication (MFA) technologies and benefit from an app such as Google or Microsoft's 'Authenticator' app.

This course is not suited for customer sites where the use of portable electronic devices (e.g. smartphones, tablets) are restricted, as the trainer will require these to manage the cloud environment.