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.

**WHAT WILL I LEARN?**

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, Google & Microsoft) and consolidate learning in a group workshop to develop a cloud security architecture, based on a realistic scenario.

**DAY ONE**

Introduction
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