Professional Cloud Security Engineer

Course Overview

The Professional Cloud Security Engineer course outline is designed to equip candidates with the skills to design, develop, and manage secure infrastructure on Google Cloud. It maps directly to the official certification exam, which consists of 50-60 multiple-choice and multiple-select questions

Course Description

This course teaches you how to design and implement a secure infrastructure on Google Cloud. You will learn about security best practices and industry compliance requirements. The training covers identity management, network security, data protection, and logging. You will also learn how to monitor threats and secure applications.
summarizes a class's core focus, target audience, and key learning outcomes. It explains what you will study and why the course is valuable.Key ComponentsCore Focus: Main topics covered in the training.Target Audience: Who should take the class.Prerequisites: Required skills before starting the course.Learning Outcomes: Skills you gain by completing it.

Learning Curriculum

Module 1

Configuring Access and Identity

Cloud Identity & Resource Hierarchy: Managing user accounts, custom roles, and service accounts. Understanding the resource hierarchy (Organizations, Folders, Projects, and Resource Manager).Authentication and Authorization: Implementing Identity and Access Management (IAM), OAuth, and Multi-Factor Authentication (MFA).Context-Aware Access & IAP: Using Identity-Aware Proxy (IAP) to establish context-aware access to applications and VM instances

Module 2

Securing Network Architectures

Network Segmentation & Perimeter Security: Architecting Virtual Private Clouds (VPCs), subnets, firewall rules, and VPC Service Controls.Private Connectivity: Configuring Cloud VPN, Cloud Interconnect, and private Google access.Traffic Inspection: Implementing Cloud Armor for DDoS protection and Web Application Firewall (WAF) rules, and Cloud NAT

Module 3

Ensuring Data Protection

Encryption at Rest: Managing Customer-Managed Encryption Keys (CMEK) and Customer-Supplied Encryption Keys (CSEK) using Cloud Key Management Service (KMS).Data Loss Prevention (DLP): Utilizing Cloud Data Loss Prevention (DLP) API to discover, classify, and protect sensitive data.Encryption in Transit: Configuring SSL/TLS for secure communication channels

Module 4

Managing Operations and Monitoring

Logging and Auditing: Implementing Cloud Logging (formerly Stackdriver) and exporting audit logs to BigQuery for analysis.Threat Detection: Utilizing Security Command Center (SCC) to identify vulnerabilities, monitor for threats, and maintain visibility over the cloud environment.

Module 5

Securing Workloads and Applications

Container and GKE Security: Securing Google Kubernetes Engine (GKE) clusters using Role-Based Access Control (RBAC), Workload Identity, Pod Security Policies, and Binary Authorization.DevSecOps: Integrating security into continuous integration and continuous deployment (CI/CD) pipelines, implementing Cloud Build security, and using vulnerability scanning

Module 6

Governance, Risk, and Compliance

Compliance Frameworks: Understanding regulatory concerns (e.g., GDPR, HIPAA, PCI-DSS) and mapping them to Google Cloud controls.Incident Response: Defining and executing incident response plans, handling incident isolation, and forensic data collection

© 2026 Proasia Upskilling Sdn Bhd | www.proasia.my