Google Cloud Professional Cloud Security Engineer Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The accelerated shift to cloud-native architectures has made securing enterprise infrastructure on the Google Cloud Platform (GCP) a critical requirement. Google Cloud Professional Cloud Security Engineer Training Course is meticulously designed to transform security, network, and cloud professionals into certified Professional Cloud Security Engineers. You will master the deployment of secure workloads, the implementation of robust Identity and Access Management (IAM), and the configuration of advanced network security defenses using Google Cloud?ÇÖs native tools. The curriculum focuses on a Zero Trust security model, leveraging cutting-edge concepts like Workload Identity Federation and Security Policy as Code to ensure comprehensive data protection and organizational compliance across all GCP services, from Compute Engine and GKE to Cloud Storage.

This program goes beyond theoretical knowledge, providing a high-impact, hands-on learning experience grounded in real-world scenarios. We delve into core domains such as data encryption with Cloud KMS/HSM, threat detection using Security Command Center, and establishing airtight security boundaries with VPC Service Controls. By completing this training, you will gain the technical expertise and strategic mindset necessary to design, develop, and manage a governed, resilient, and compliant cloud environment, effectively mitigating risk and establishing a future-proof security posture for any organization utilizing the powerful, global infrastructure of Google Cloud.

Programme Curriculum

Google Cloud Professional Cloud Security Engineer Training Course

Introduction

The accelerated shift to cloud-native architectures has made securing enterprise infrastructure on the Google Cloud Platform (GCP) a critical requirement. Google Cloud Professional Cloud Security Engineer Training

Course is meticulously designed to transform security, network, and cloud professionals into certified Professional Cloud Security Engineers. You will master the deployment of secure workloads, the implementation of robust Identity and Access Management (IAM), and the configuration of advanced network security defenses using Google Cloud?ÇÖs native tools. The curriculum focuses on a Zero Trust security model, leveraging cutting-edge concepts like Workload Identity Federation and Security Policy as Code to ensure comprehensive data protection and organizational compliance across all GCP services, from Compute Engine and GKE to Cloud Storage.

This program goes beyond theoretical knowledge, providing a high-impact, hands-on learning experience grounded in real-world scenarios. We delve into core domains such as data encryption with Cloud KMS/HSM, threat detection using Security Command Center, and establishing airtight security boundaries with VPC Service Controls. By completing this training, you will gain the technical expertise and strategic mindset necessary to design, develop, and manage a governed, resilient, and compliant cloud environment, effectively mitigating risk and establishing a future-proof security posture for any organization utilizing the powerful, global infrastructure of Google Cloud.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Configure and administer a Zero Trust security model on GCP using the principle of least privilege.
2. Implement and manage Identity and Access Management (IAM) with custom roles and Workload Identity Federation.
3. Design and enforce secure Organizational Policy constraints across the GCP resource hierarchy.
4. Establish robust VPC Service Controls to create a secure perimeter for sensitive services and data.
5. Apply advanced Network Security Defenses, including Cloud Firewall, Cloud Armor, and IDS to protect cloud workloads.
6. Ensure Data Protection at rest and in transit using Cloud KMS, CMEK/CSEK, and Secret Manager.
7. Secure containerized workloads by implementing Google Kubernetes Engine (GKE) Security best practices, including Binary Authorization.
8. Design and deploy effective Threat Detection and Vulnerability Management using Security Command Center.
9. Configure Cloud Logging and Monitoring solutions for comprehensive security auditing and log analysis.
10. Manage security for hybrid and multi-cloud environments utilizing Workload Identity Federation.
11. Implement DevSecOps principles by integrating security checks into CI/CD pipelines.
12. Support and enforce complex Compliance Requirements like HIPAA, PCI DSS, and ISO 27001 on GCP.
13. Design secure reference architectures for services like BigQuery and Cloud Storage with strong encryption controls.

Target Audience

1. Existing Cloud Security Engineers.
2. Security Analysts/Architects.
3. Network Engineers.
4. DevSecOps Engineers.
5. IT Professionals preparing for the Google Cloud Professional Cloud Security Engineer Certification.
6. Compliance and Risk Officers.

7. System Administrators.
8. Cloud Architects.

Course Modules

Module 1: GCP Security Foundations and Shared Responsibility

- Understanding the Shared Responsibility Model in a cloud environment.
- Implementing the GCP Resource Hierarchy for effective policy management.
- Configuring Organization Policies and constraints for enterprise governance.
- Introduction to the Google Cloud Security Command Center dashboard.
- Case Study: Analyzing the root cause of a cloud misconfiguration breach and how an Organization Policy constraint could have prevented it.

Module 2: Core Identity and Access Management (IAM)

- Mastering the Principle of Least Privilege using IAM roles
- Configuring and auditing Service Accounts and their keys/Workload Identity.
- Implementing Identity-Aware Proxy (IAP) for securing application access.
- Integrating external identities using Workload Identity Federation.
- Case Study: Securing third-party vendor access to a development project using a temporary, federated identity and IAP instead of long-lived service account keys.

Module 3: Network Security Defenses - VPC and Firewall

- Designing secure Virtual Private Cloud network architectures and subnets.
- Configuring fine-grained VPC Firewall Rules using tags and service accounts.
- Implementing Private Google Access for enhanced security.
- Understanding and configuring VPC Peering and Shared VPC securely.
- Case Study: Designing a multi-region, three-tier application architecture with micro-segmentation enforced by Service Account-based firewall rules to prevent lateral movement.

Module 4: Perimeter Defense with VPC Service Controls

- Establishing an effective Security Perimeter to safeguard sensitive services.
- Configuring Access Levels and Access Context Manager policies.
- Implementing and troubleshooting VPC SC security boundaries.
- Protecting data in services like BigQuery and Cloud Storage from exfiltration.
- Case Study: Simulating and mitigating a data exfiltration attempt from a BigQuery dataset by enforcing an ingress/egress policy using a VPC Service Control perimeter.

Module 5: Data Protection and Encryption

- Implementing Data Classification and data handling best practices on GCP.
- Managing encryption keys using Cloud Key Management Service
- Utilizing Customer-Managed Encryption Keys and Customer-Supplied Encryption Keys.
- Securely storing secrets and sensitive credentials with Secret Manager.
- Case Study: Designing and implementing a key rotation policy for a high-compliance database using a dedicated Cloud HSM key ring to meet regulatory requirements.

Module 6: Securing Compute Engine Workloads

- Hardening Compute Engine instances and images
- Configuring secure metadata and startup scripts.
- Implementing Managed Instance Groups for security and resilience.
- Leveraging VPC Flow Logs for network traffic analysis and anomaly detection.
- Case Study: Applying a security checklist to harden a newly provisioned web server VM instance, including enabling Shielded VM features and securing administrative access via IAP TCP Forwarding.

Module 7: Google Kubernetes Engine (GKE) Security

- Understanding the GKE Shared Responsibility Model and control plane security.
- Securing the Node Pool
- Implementing Network Policy for pod-to-pod isolation.
- Enforcing deployment security with Binary Authorization and admission controllers.
- Case Study: Implementing a secure, private GKE cluster architecture, showing how to enforce policy-based deployment using Binary Authorization to restrict container image sources.

Module 8: Serverless and Application Security

- Securing Cloud Functions, Cloud Run, and App Engine environments.
- Implementing Cloud Endpoints and API Keys for managed API access.
- Protecting applications against web attacks using Cloud Armor.
- Integrating reCAPTCHA Enterprise for bot and fraud prevention.
- Case Study: Defending a public-facing Cloud Run service against common OWASP Top 10 attacks by configuring a Cloud Armor security policy and WAF rules.

Module 9: Cloud Data Loss Prevention (DLP)

- Inspecting and transforming sensitive data using Cloud DLP for PII/PHI.
- Configuring De-identification techniques
- Scanning and classifying sensitive data within Cloud Storage and BigQuery.
- Integrating DLP into Data Pipeline workflows for automated compliance.
- Case Study: Developing a pipeline that automatically scans incoming log files in a Cloud Storage bucket, redacts credit card numbers using DLP, and stores the de-identified data in BigQuery.

Module 10: Security Operations, Logging, and Monitoring

- Configuring Cloud Audit Logs and understanding log types
- Utilizing Cloud Logging and Cloud Monitoring for security observability.
- Creating security-specific Alerting Policies for critical events
- Implementing Log Sinks for exporting security logs to SIEM/external tools.
- Case Study: Setting up a centralized logging export solution to a third-party SIEM and creating a custom alert to detect the deletion of a production Cloud SQL instance.

Module 11: Threat Detection and Incident Response

- Leveraging Security Command Center for continuous security posture management.
- Prioritizing and responding to findings from SCC
- Understanding the Risk Management Framework and best practices for incident response on GCP.
- Automating security response using Cloud Functions and Pub/Sub triggers.
- Case Study: Responding to a high-severity finding in Security Command Center related to a publicly exposed Cloud Storage bucket and automating remediation actions.

Module 12: Compliance and Governance

- Mapping GCP controls to Industry Compliance Standards
- Understanding and using Access Transparency and Access Approval.
- Implementing security controls for regulated workloads
- Conducting security assessments and continuous compliance checks.
- Case Study: Reviewing a financial services company's compliance requirements and verifying the implementation of required technical controls on their GCP environment for PCI DSS.

Module 13: DevSecOps and Security Automation

- Integrating security testing into the CI/CD pipeline
- Utilizing Cloud Build and Artifact Registry security features.
- Automating infrastructure security with Terraform/Deployment Manager and policy checks.
- Applying security to Infrastructure as Code (IaC) templates.
- Case Study: Automating the deployment of a new VPC network using Terraform, ensuring pre-deployment policy checks (linter) prevent the creation of overly permissive firewall rules.

Module 14: Advanced Network Security Services

- Configuring Cloud Load Balancing security features
- Deploying Cloud NAT securely.
- Understanding and configuring Cloud VPN/Cloud Interconnect for hybrid security.
- Implementing a secure DNS Policy with Cloud DNS.
- Case Study: Securing a high-traffic e-commerce front end by placing it behind a Global HTTP(S) Load Balancer with a Cloud Armor WAF policy to mitigate SQL injection attacks.

Module 15: Exam Preparation and Review

- Comprehensive review of the official Professional Cloud Security Engineer exam guide.
- Strategy session for tackling scenario-based and multi-select questions.
- Final Full-Length Mock Exam simulation and detailed answer review.
- Case Study: An architectural review of a fully secured, enterprise-scale reference environment, synthesizing all key security components into a holistic defense-in-depth strategy.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com