Google Cloud Certified Professional Cloud Security Engineer

Course Outline:

Section 1: Configuring access within a cloud solution environment

1.1 Configuring Cloud Identity. Considerations include:

- Managing Cloud Identity
- Configuring Google Cloud Directory Sync
- Management of super administrator account

1.2 Managing user accounts. Considerations include:

- Designing identity roles at the project and organization level
- Automation of user lifecycle management process
- API usage

1.3 Managing service accounts. Considerations include:

- Auditing service accounts and keys
- Automating the rotation of user managed service account keys

- Creating, authorizing and securing service accounts
- Securely managed API access management

1.4 Managing authentication. Considerations include:

- Creating a password policy for user accounts
- Establishing Security Assertion Markup Language (SAML)
- Configuring and enforcing two-factor authentication

1.5 Managing and implementing authorization controls. Considerations include:

- Using Resource Hierarchy for Access Control
- Privileged roles and separation of duties
- Managing IAM permissions with primitive, predefined, and custom roles
- Granting permissions to different types of identities
- Understanding difference between Google Cloud Storage IAM and ACLs

1.6 Defining Resource Hierarchy. Considerations include:

- Creating and managing organizations
- Resource structures (orgs, folders and projects)
- Defining and managing Organization constraints
- Using Resource Hierarchy for Access Control and permissions inheritance
- Trust and security boundaries within GCP projects

Section 2: Configuring network security

2.1 Designing network security. Considerations include:

- Security properties of a VPC Network, VPC Peering, Shared VPC, and Firewall Rules
- Network isolation and data encapsulation for N tier application design
- Use of DNSSEC
- Private vs. public addressing
- App-to-app security policy

2.2 Configuring network segmentation. Considerations include:

- Network perimeter controls (firewall rules; IAP)
- Load balancing (global, network, HTTP(S), SSL Proxy, and TCP Proxy load balancers)

2.3 Establish private connectivity. Considerations include:

- Private RFC1918 connectivity between VPC networks and GCP Projects (Shared VPC, VPC Peering)
- Private RFC1918 connectivity between data centers and VPC network (IPSEC and Cloud Interconnect).
- Enable private connectivity between VPC and Google APIs (Private Access)

Section 3: Ensuring data protection

3.1 Preventing data loss with the DLP API. Considerations include:

- Identification and redaction of PII
- Configuring tokenization
- Configure format preserving substitution
- Restricting access to DLP Datasets

3.2 Managing encryption at rest. Considerations include:

- Understanding use cases for Default Encryption, Customer-Managed Encryption Keys (CMEK), and Customer-Supplied Encryption Keys (CSEK)
- Creating and managing encryption keys for CMEK and CSEK
- Managing application secrets
- Object lifecycle policies for Cloud Storage
- Enclave computing
- Envelope encryption

Section 4: Managing operations within a cloud solution environment

4.1 Building and deploying infrastructure. Considerations include:

- Backup and data loss strategy
- Creating and automating an incident response plan
- Log sinks, audit logs, and data access logs for near-realtime monitoring
- Standby models
- Automate security scanning for Common Vulnerabilities and Exploits (CVEs) through a CI/CD pipeline
- Virtual machine image creation, hardening and maintenance
- Container image creation, hardening, maintenance, and patch management

4.2 Building and deploying applications. Considerations include:

- Application logs near-realtime monitoring
- Static code analysis
- Automate security scanning through a CI/CD pipeline

4.3 Monitoring for security events. Considerations include:

- Logging, monitoring, testing and alerting for security incidents
- Exporting logs to external security systems
- Automated and manual analysis of access logs
- Understanding capabilities Cloud Security Scanner and Forseti

Section 5: Ensuring compliance

5.1 Comprehension of regulatory concerns. Considerations include:

- Evaluation of concerns relative to compute, data, and network.
- Security shared responsibility model
- Security guarantees within cloud execution environments
- Limiting compute and data for regulatory compliance

5.2 Comprehension of compute environment concerns. Considerations include:

- Security guarantees and constraints for each compute environment (Compute Engine, Kubernetes Engine, App Engine)
- Determining which compute environment is appropriate based on company compliance standards

Source: https://cloud.google.com/certification/cloud-security-engineer