Section - 3

Security Best Practices in Google Cloud

3.1 Introduction to Security in Google Cloud

Explanation:

Security is a **shared responsibility** in Google Cloud:

- Google secures the infrastructure.
- Users must secure configurations, identity, data, and workloads.

Key pillars of cloud security:

- Identity and Access Management (IAM)
- Data Protection
- Network Security
- Threat Detection and Response
- Compliance

Real-world Example:

A healthcare company uses Google Cloud's encryption services to meet HIPAA compliance for patient data.

3.2 Identity and Access Management (IAM) Best Practices

Explanation:

IAM is the first line of defense. Poor IAM configurations are the #1 cause of cloud breaches.

Best Practices:

- **Principle of Least Privilege:** Assign the minimum permissions necessary.
- **Use Predefined Roles:** Instead of custom roles where possible.
- **Service Accounts:** Use different service accounts for different applications.
- **Audit Logs:** Regularly monitor who accesses what.

Real-world Example:

A FinTech firm uses custom IAM roles to restrict access so that developers can deploy applications but cannot modify network configurations.

3.3 Securing Google Kubernetes Engine (GKE)

Best Practices:

- **Private Clusters:** Only internal IPs for nodes and control plane.
- **Workload Identity:** Bind Kubernetes Service Accounts to GCP Service Accounts securely.
- **Pod Security Policies / GKE Autopilot:** Enforce restrictions on what pods can do.

Real-world Example:

A media streaming company uses private GKE clusters with firewall rules limiting access to only authorized admin IPs.

3.4 Protecting Data at Rest and In Transit

Explanation:

- **Data at Rest:** Encrypt using Google-managed or Customer-managed encryption keys (CMEK).
- **Data in Transit:** Default TLS/SSL encryption for data moving between GCP services.

Real-world Example:

A retail company encrypts all BigQuery datasets with customer-supplied encryption keys (CSEK) for regulatory compliance.

3.5 Secure Network Architecture

Best Practices:

- **VPC Service Controls:** Define perimeters to prevent data exfiltration.
- **Firewall Rules:** Deny all by default, then allow as needed.
- **Private Access:** Use Private Google Access for serverless services and GKE.

Real-world Example:

A biotech company builds an isolated network perimeter using VPC Service Controls around sensitive research data storage.

3.6 Using Security Command Center (SCC)

Explanation:

Google Cloud Security Command Center provides centralized visibility into risks.

Capabilities:

- Detect misconfigurations
- Identify vulnerabilities
- Monitor compliance violations

Real-world Example:

A transportation startup uses SCC to detect and fix misconfigured Cloud Storage buckets exposing data to the public.

3.7 Logging and Monitoring for Security

Best Practices:

- Enable **Cloud Audit Logs** for every service.
- Use **Cloud Monitoring** and **Cloud Logging** for alerts and dashboards.
- Integrate with **SIEMs** like Splunk or Chronicle for centralized threat detection.

Real-world Example:

A bank integrates GCP logs with Splunk to monitor unauthorized login attempts across its applications.

3.8 Threat Detection with Google Cloud Armor and BeyondCorp

Google Cloud Armor:

- Protects applications from DDoS attacks and common exploits like SQL injection.

BeyondCorp:

- Implements a **zero-trust** security model: "Never trust, always verify."

Real-world Example:

A government agency uses BeyondCorp to allow employees to access internal apps securely without VPNs.