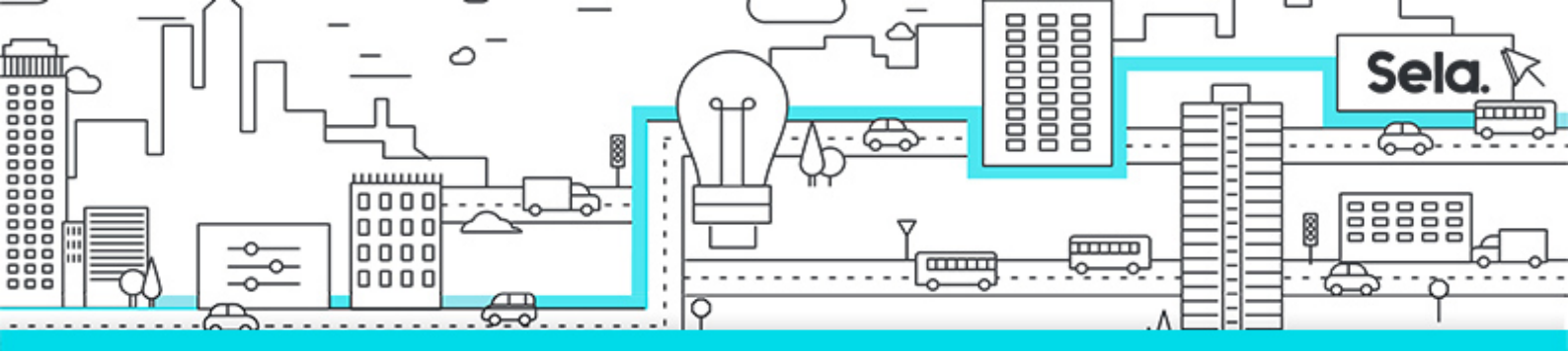
GCPSecBP

# Security Best Practives in Google Cloud

college@sela.co.il 03-6176666




# Security Best Practives in Google Cloud

GCPSecBP - Version: 1

## 5 days course

**Description:**

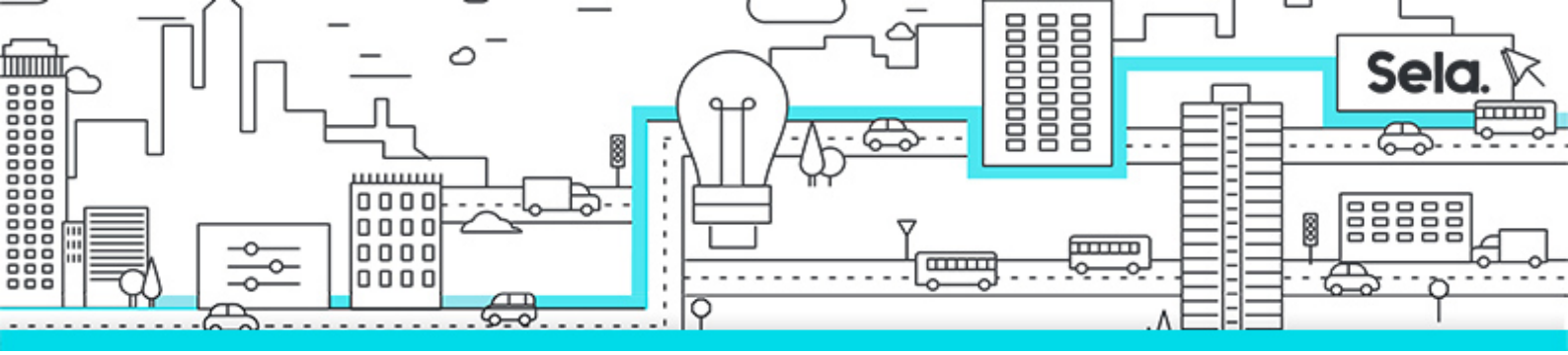
This self-paced training course gives participants broad study of security controls and techniques on Google Cloud. Through recorded lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure Google Cloud solution, including Cloud Storage access control technologies, Security Keys, Customer-Supplied Encryption Keys, API access controls, scoping, shielded VMs, encryption, and signed URLs. It also covers securing Kubernetes environments.

**Intended Audience:**

[Cloud] information security analysts, architects, and engineers. Information security/cybersecurity specialists. Cloud infrastructure architects. Also intended for Google and partner field personnel who work with customers in those job roles. Also useful for cloud application developers.

**Prerequisites:**

• Prior completion of Google Cloud Fundamentals: Core Infrastructure or equivalent experience. Prior completion of Networking in Google Cloud or equivalent experience. Knowledge of foundational concepts in information security: Fundamental concepts: vulnerability, threat, attack surface confidentiality, integrity, availability, Common threat types and their mitigation strategies, Public-key cryptography, Public and private key pairs, Certificates Cipher types, Key width Certificate authorities, Transport Layer Security/Secure Sockets, Layer encrypted communication Public key infrastructures Security




policy. Basic proficiency with command-line tools and Linux operating system environments. Systems Operations experience, including deploying and managing applications, either on-premises or in a public cloud environment. Reading comprehension of code in Python or JavaScript.

**Objectives:**

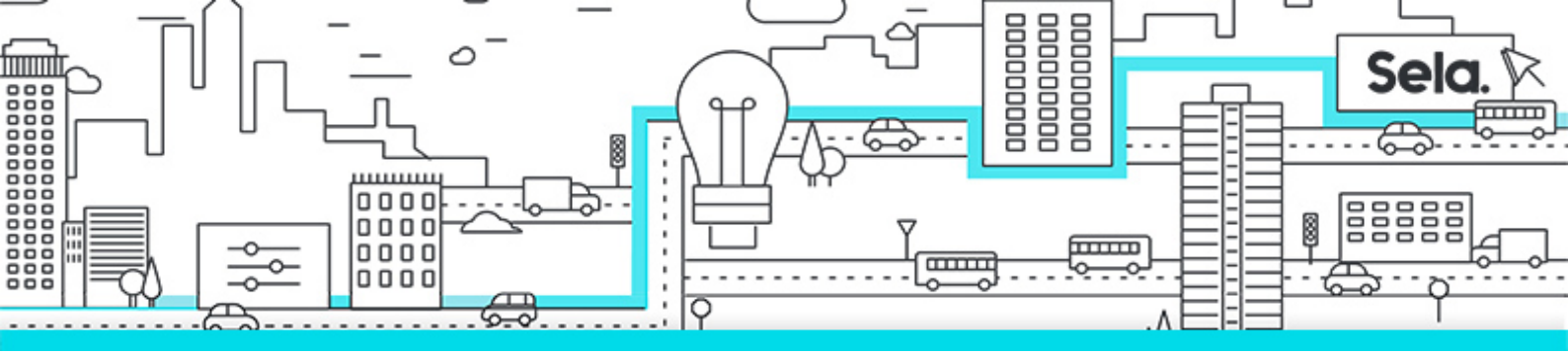
- Apply techniques and best practices to secure Compute Engine
- Apply techniques and best practices to secure cloud data
- Apply techniques and best practices to secure applications
- Apply techniques and best practices to secure Kubernetes

**Topics:**

- **Welcome to Security Best Practices in Google Cloud**

- **Securing Compute Engine: Techniques and Best Practices**
  - Module Overview
  - Service accounts, IAM roles, and API scopes
  - Lab Intro: Configuring, Using, and Auditing VM Service Accounts and Scopes
  - Getting Started with Google Cloud and Qwiklabs
  - Connecting to virtual machines
  - Connecting to VMs without external IPs
  - OS Login
  - Organization policy controls
  - Shielded VMs
  - Confidential VMs
  - Certificate Authority Service
  - What Certificate Authority Service provides
  - Compute Engine best practices
  - Module review

- **Securing Cloud Data: Techniques and Best Practices**



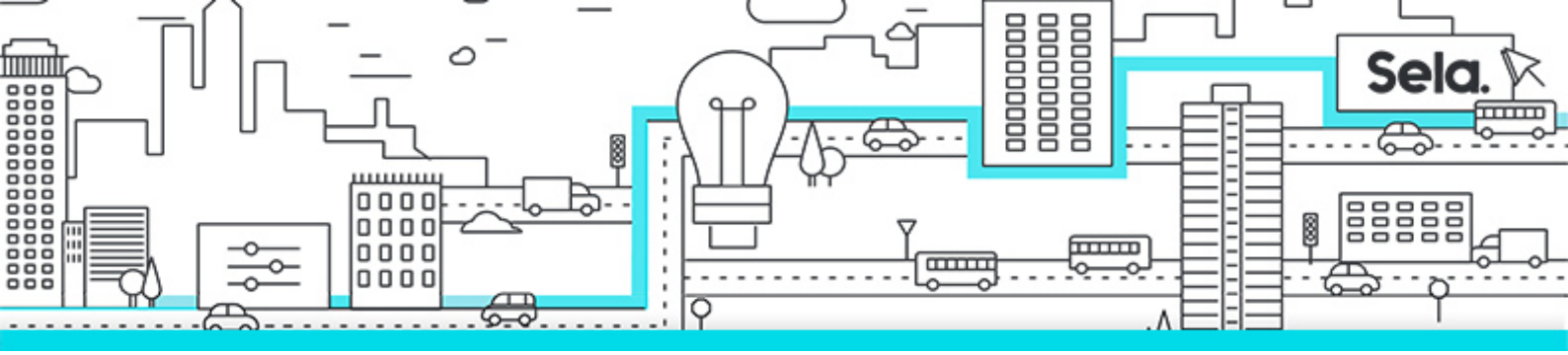

- Module Overview1m
- Cloud Storage IAM permissions and ACLs
- Auditing cloud data
- Signed URLs and policy documents
- Encrypting with CMEK and CSEK
- Lab Intro: Using Customer-Supplied Encryption Keys with Cloud Storage
- Lab Intro: Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS
- Demo: Using and Verifying Keys in Cloud HSM
- BigQuery IAM Roles and Authorized Views
- Lab Intro: Creating a BigQuery Authorized View2
- Storage best practices
- Module Review

**• Application Security: Techniques and Best Practices**

- Module Overview
- Types of application security vulnerabilities
- Web Security Scanner
- Lab Intro: Using Web Security Scanner to Find Vulnerabilities in an App Engine Application
- Threat: Identity and Oauth phishing
- Identity-Aware Proxy (IAP)
- Lab Intro: Securing Compute Engine Applications with BeyondCorp Enterprise
- Secret Manager
- Lab Intro: Configuring and Using Credentials with Secret Manager
- Module review

**• Securing Google Kubernetes Engine: Techniques and Best Practices**

- Module Overview
- Introduction to Kubernetes/GKE
- Authentication and authorization
- Hardening your Clusters




- Securing Your Workloads
- Monitoring and logging
- Module review