

Sela.

GCP_SGC

Security in Google Cloud

college@sela.co.il

03-6176666





Security in Google Cloud

GCP_SGC - Version: 1

 3 days Course

Description:

This training course gives you a broad study of security controls and techniques in Google Cloud. Through recorded lectures, demonstrations, and hands-on labs, you'll explore and deploy the components of a secure Google Cloud solution, including Cloud Identity, Resource Manager, Identity and Access Management (IAM), Virtual Private Cloud firewalls, Cloud Load Balancing, Direct Peering, Carrier Peering, Cloud Interconnect, and VPC Service Controls.

Intended audience:

- Cloud information security analysts, architects, and engineers
- Information security/cybersecurity specialists
- Cloud infrastructure architects

Prerequisites:

- Prior completion of Google Cloud Fundamentals: Core Infrastructure or equivalent experience
- Prior completion of Networking in Google Cloud or equivalent experience
- Basic understanding of Kubernetes terminology (preferred but not required)
- Knowledge of foundational concepts in information security, through experience or through online training such as SANS's SEC301: Introduction to Cyber Security
- 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:

- Understand Google's approach to security.
- Manage administration identities using Cloud Identity.
- Implement least privilege administration using Resource Manager and IAM.
- Implement Identity-Aware Proxy.
- Implement IP traffic controls using VPC firewalls and Google Cloud Armor.
- Remediate security vulnerabilities, especially public access to data and virtual machines.
- Scan for and redact sensitive data using the Cloud Data Loss Prevention API.
- Analyze changes to resource metadata configuration using audit logs.
- Scan a Google Cloud deployment with Forseti, to remediate important types of vulnerabilities, especially in public access to data and VMs.

Topics:

Foundations of Google Cloud Security

- • Google Cloud's Approach to Security
- • The Shared Security Responsibility Model
- • Threats Mitigated by Google and Google Cloud



- • Access Transparency

Cloud Identity

- • Cloud Identity
- • Google Cloud Directory Sync
- • Google Authentication Versus SAML-based SSO
- • Authentication Best Practices

Identity and Access Management (IAM)

- • Resource Manager
- • IAM Roles
- • IAM Policies
- • IAM Recommender
- • IAM Troubleshooter
- • IAM Audit Logs
- • IAM Best Practices

Configuring Virtual Private Cloud for Isolation and Security

- • VPC Firewalls
- • Load Balancing and SSL Policies
- • Interconnect and Peering Policies
- • Best Practices for VPC Networks
- • VPC Flow Logs

Securing Compute Engine: Techniques and Best Practices

- • Service Accounts, IAM Roles and API Scopes



- • Managing VM Logins
- • Organization Policy Controls
- • Compute Engine Best Practices
- • Encrypting Disks with CSEK

Securing Cloud Data: Techniques and Best Practices

- • Cloud Storage IAM permissions and ACLs
- • Auditing Cloud Data
- • Signed URLs and Policy Documents
- • Encrypting with CMEK and CSEK
- • Cloud HSM
- • BigQuery IAM Roles and Authorized Views
- • Storage Best Practices

Application Security: Techniques and Best Practices

- • Types of Application Security Vulnerabilities
- • Web Security Scanner
- • Threat: Identity and Oauth Phishing
- • Identity-Aware Proxy
- • Secret Manager

Securing Google Kubernetes Engine: Techniques and Best Practices

- • Introduction to Kubernetes/GKE
- • Authentication and Authorization
- • Hardening Your Clusters
- • Securing Your Workloads
- • Monitoring and Logging



Protecting against Distributed Denial of Service Attacks (DDoS)

- • How DDoS Attacks Work
- • Google Cloud Mitigations
- • Types of Complementary Partner Products

Content-Related Vulnerabilities: Techniques and Best Practices

- • Threat Ransomware
- • Ransomware Mitigations
- • Threats: Data Misuse, Privacy Violations, Sensitive Content
- • Content-Related Mitigations

Monitoring, Logging, Auditing, and Scanning

- • Cloud Audit Logs
- • Deploying and Using Forseti