Security in Google Cloud

Overview

This course gives participants broad study of security controls and techniques on Google Cloud Platform. Through lectures, demonstrations, and hands-on labs, participants explore and deploy the components of a secure Google Cloud solution. Participants also learn mitigation techniques for attacks at many points in a Google Cloud-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Prerequisite Comments

To get the most out of this course, participants should have:
Prior completion of Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience
Prior completion of Networking in Google Cloud Platform 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

Target Audience

This class is intended for the following job roles:
[Cloud] information security analysts, architects, and engineers
Information security/cybersecurity specialists
Cloud infrastructure architects Additionally, the course is intended for Google and partner field personnel who work with customers in those job roles.
The course should also be useful to developers of cloud applications

Course Objectives

This course teaches participants the following skills:
Understanding the Google approach to security Managing administrative identities using Cloud Identity.
Implementing least privilege administrative access using Google Cloud Resource Manager, Cloud IAM.
Implementing IP traffic controls using VPC firewalls and Cloud Armor Implementing Identity Aware Proxy Analyzing changes to the configuration or metadata of

resources with GCP audit logs Scanning for and redact sensitive data with the Data Loss Prevention API Scanning a GCP deployment with Forseti Remediating important types of vulnerabilities, especially in public access to data and VMs

Course Outline

1 - Foundations of GCP Security

Google Cloud's approach to security
The shared security responsibility model
Threats mitigated by Google and by GCP
Access Transparency

2 - Cloud Identity

Cloud Identity
Syncing with Microsoft Active Directory
Choosing between Google authentication and SAML-based SSO
GCP best practices

3 - Identity and Access Management

GCP Resource Manager: projects, folders, and organizations
GCP IAM roles, including custom roles
GCP IAM policies, including organization policies
GCP IAM best practices

4 - Configuring Google Virtual Private Cloud for Isolation and Security

Configuring VPC firewalls (both ingress and egress rules)
Load balancing and SSL policies
Private Google API access
SSL proxy use
Best practices for structuring VPC networks
Best security practices for VPNs
Security considerations for interconnect and peering options
Available security products from partners

5 - Monitoring, Logging, Auditing, and Scanning

Stackdriver monitoring and logging
VPC flow logs
Cloud audit logging
Deploying and Using Forseti

6 - Securing Compute Engine: techniques and best practices

Compute Engine service accounts, default and customer-defined
IAM roles for VMs
API scopes for VMs
Managing SSH keys for Linux VMs
Managing RDP logins for Windows VMs
Organization policy controls: trusted images, public IP address, disabling serial port
Encrypting VM images with customer-managed encryption keys and with customer-supplied encryption keys
Finding and remediating public access to VMs
VM best practices
Encrypting VM disks with customer-supplied encryption keys

7 - Securing cloud data: techniques and best practices

Cloud Storage and IAM permissions
Cloud Storage and ACLs
Auditing cloud data, including finding and remediating publicly accessible data
Signed Cloud Storage URLs
Signed policy documents
Encrypting Cloud Storage objects with customer-managed encryption keys and with customer-supplied encryption keys
Best practices, including deleting archived versions of objects after key rotation
BigQuery authorized views
BigQuery IAM roles
Best practices, including preferring IAM permissions over ACLs

8 - Protecting against Distributed Denial of Service Attacks: techniques and best practices

How DDoS attacks work
Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Cloud Armor
Types of complementary partner products

9 - Application Security: techniques and best practices

Types of application security vulnerabilities
DoS protections in App Engine and Cloud Functions
Cloud Security Scanner
Threat: Identity and Oauth phishing
Identity Aware Proxy

10 - Content-related vulnerabilities: techniques and best practices

Threat: Ransomware
Mitigations: Backups, IAM, Data Loss Prevention API
Threats: Data misuse, privacy violations, sensitive/restricted/unacceptable content
Mitigations: Classifying content using Cloud ML APIs; scanning and redacting data using Data Loss Prevention API

Related Courses, Certifications, Exams

- Networking in Google Cloud
- Google Cloud Fundamentals - Core Infrastructure