Security in Google Cloud

Course 4325– 24 Hours

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 GCP solution. Participants also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

On Completion, Delegates will be able to

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

Who Should Attend

Cloud information security analysts, architects, and engineers

Information security/cybersecurity specialists

Cloud infrastructure architects

Developers of cloud applications

Prerequisites

- Prior completion of Google Cloud Fundamentals: Core Infrastructure course 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

Course Contents

PART I: Managing Security In Google Cloud

Module 1: Foundations of GCP Security

Securing systems is a hot topic and should be a priority for everyone today - and, as you will see, it is definitely a priority here at Google. In this module we will introduce you to Google Cloud's approach to security. We will also discuss the shared security responsibility model, which is a collaborative effort between Google and its users. Next, we will outline several threats that are mitigated for you when your systems are run on Google's infrastructure in Google Cloud. And, finally, we will end with a section on access transparency.

Module 2: Cloud Identity

In this module we will discuss Cloud Identity, a service which makes it easy to manage cloud users, devices, and apps from one console. We will also discuss a few related features to help

reduce the operational overhead of managing Google Cloud users, such as the Google Cloud Directory Sync and Single Sign-On. We will end with some authentication best practices.

Module 3: Identity, Access, and Key Management

Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage your cloud resources centrally. More specifically, we will cover; the Resource Manager which enables you to centrally manage projects, folders, and organizations, IAM roles and policies, including custom roles, and IAM best practices, including separation of duties and the principle of least privilege.

Module 4: Configuring Google Virtual Private Cloud for Isolation and Security

Managed networking on Google Cloud utilizes a Virtual Private Cloud (or VPC). In this module we will discuss VPC related security concepts including: VPC firewalls, load balancing SSL policies, network Interconnect & peering options, VPC network best practices and VPC flow logs. You will also have the opportunity to practice what you've learned, by completing the labs exercises "Configuring VPC Firewalls" and "Configuring and Using VPC Flow Logs in Cloud Logging."

PART II: Security Best Practices in Google Cloud

Module 5: Securing Compute Engine: techniques and best practices

In this module we will start with a discussion of service accounts, IAM roles and API scopes as they apply to compute engine. We will also discuss managing VM logins, and how to use organization policies to set constraints that apply to all resources in your organization's hierarchy. Next, we will review compute engine best practices to give you some tips for securing compute engine.Lastly, we will cover encrypting persistent disks with Customer-Supplied Encryption keys.

Module 6: Securing cloud data: techniques and best practices

In this module we discuss controlling IAM permissions and access control lists on Cloud Storage buckets, auditing cloud data, including finding and remediating data that has been set to publicly accessible, how to use signed Cloud Storage URLs and signed policy documents, and encrypting data at rest. In addition, BigQuery IAM roles and authorized views will be covered to demonstrate managing access to datasets and tables. The module will conclude with an overview of storage best practices

Module 7: Application Security: Techniques and Best Practices

In this module we will discuss application security techniques and best practices. We will see how Web Security Scanner can be used to identify vulnerabilities in your applications, and dive into the subject of Identity and Oauth phishing. Lastly, you will learn how Identity-Aware Proxy, or IAP, can be used to control access to your cloud applications.

Module 8: Securing Kubernetes: Techniques and Best Practices

Protecting workloads in Google Kubernetes Engine involves many layers of the stack, including the contents of your container image, the container runtime, the cluster network, and access to the cluster API server. In this module, you will learn how to securely set up your Authentication and Authorization, how to harden your clusters, secure your workloads, and monitor everything to make sure it stays in good health.

PART III: Mitigating Security Vulnerabilities on Google Cloud

Module 9: Protecting against Distributed Denial of Service Attacks (DDoS)

Distributed Denial of Service Attacks are a major concern today and can have a huge impact on businesses if the business is not adequately prepared. In this module we will begin with a quick discussion on how DDoS attacks work and then review some DDoS mitigation techniques that are provided by Google Cloud. We will finish up with a review of complementary partner products and a lab where you will get a chance to see some DDoS mitigations in action.

Module 10: Content-Related Vulnerabilities: Techniques and Best Practices

In this module we will discuss threats to your content. First, we review the threat of ransomware, and some of the mitigations you can utilize in Google Cloud to help protect your systems from it. Then we will move to a discussion of threats related to data misuse and privacy violations and discuss a few mitigation strategies that can be utilized to protect applications and systems.

Module 11: Monitoring, Logging, Auditing, and Scanning

Collecting, processing, aggregating, and displaying real-time quantitative data is helpful in supplying raw input into business analytics and in facilitating analysis of security breaches. Google Cloud provides many services and features to help with this - and that is what this module is all about.In this module we will investigate Cloud Monitoring and Cloud Logging, Cloud Audit Logs, and then discuss how to leverage Forseti Security to systematically monitor your Google Cloud resources.