GCPSecurity Best Practices

Security Best Practices in Google Cloud

college@sela.co.il 03-6176666

Security Best Practices in Google Cloud

GCPSecurity Best Practices - 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

• Welcome to Security Best Practices in Google Cloud! In this course we will build upon the foundations laid during the earlier course in this series, Managing Security in Google Cloud. In this section, expect to learn more about how to implement security "best practices" to lower the risk of malicious attacks against your systems, software and data.

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.

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

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.

Securing Google Kubernetes Engine: 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.

Course Resources

• PDF links to all modules