



# Security in Google Cloud

## Course description

Learn to Secure Google Cloud Infrastructure, Applications, Data, Networks, and Kubernetes Workloads using Google Cloud Security Services and Best Practices.

- Course level: Intermediate
- Duration: 3 days

## Activities

This course includes instructor-led sessions, on-demand learning modules, hands-on labs, security demonstrations, threat mitigation workshops, cloud security assessments, and monitoring and auditing exercises to reinforce learning.

## Course objectives

In this course, you will learn to:

- Understand the foundations of Google Cloud security.
- Implement secure identity and access management practices.
- Secure VPC networks, compute workloads, and cloud data.
- Protect applications and Kubernetes environments.
- Configure DDoS mitigation and content security controls.
- Implement logging, monitoring, auditing, and scanning solutions.

- Apply security best practices across Google Cloud environments.

## **Key features**

- Google Cloud Security Foundations
- Identity and Access Management
- Secure Networking and VPC Protection
- Compute and Infrastructure Security
- Data Security and Encryption
- Application and API Security
- Kubernetes and Container Security
- Threat Protection, Monitoring, and Automation

## **Intended audience**

This course is intended for:

- Cloud Security Analysts
- Security Architects
- Security Engineers
- Cloud Infrastructure Architects
- Cybersecurity Specialists

## **Prerequisites**

We recommend that attendees of this course have:

- Google Cloud Fundamentals: Core Infrastructure
- Logging, Monitoring, and Observability in Google Cloud

## **Products covered**

- Cloud Identity
- IAM
- Cloud HSM
- Secret Manager
- Google Kubernetes Engine

- Managed Microsoft AD
- Cloud Interconnect
- Cloud Storage
- Web Security Scanner
- Identity-Aware Proxy
- VPC Service Controls
- Security Command Center
- Cloud Armor
- Cloud IDS
- Cloud DNS
- BeyondCorp Enterprise
- Certificate Authority Service

## Course outline

### **Module 01 - Foundations of Google Cloud Security**

- Google Cloud Security Approach
- Shared Security Responsibility Model
- Threat Mitigation
- Access Transparency

### **Module 02 - Securing Access to Google Cloud**

- Cloud Identity
- Google Cloud Directory Sync
- Managed Microsoft AD
- SAML-based SSO
- Identity Platform
- Authentication Best Practices

### **Module 03 - Identity and Access Management (IAM)**

- Resource Manager
- IAM Roles
- Service Accounts
- IAM Policies

- Workload Identity Federation
- Policy Intelligence

## **Module 04 - Configuring Virtual Private Cloud for Isolation and Security**

- VPC Firewalls
- Load Balancing and SSL Policies
- Cloud Interconnect
- VPC Network Peering
- VPC Service Controls
- Access Context Manager
- VPC Flow Logs
- Cloud IDS

## **Module 05 - Securing Compute Engine: Techniques and Best Practices**

- Service Accounts and API Scopes
- Managing VM Logins
- Organization Policy Controls
- Shielded VMs
- Confidential VMs
- Certificate Authority Service

## **Module 06 - Securing Cloud Data: Techniques and Best Practices**

- Cloud Storage IAM and ACLs
- Signed URLs
- CMEK and CSEK
- Cloud HSM
- BigQuery Authorized Views
- Storage Best Practices

## **Module 07 - Securing Applications: Techniques and Best Practices**

- Application Security Vulnerabilities
- Web Security Scanner

- OAuth and Identity Phishing
- Identity-Aware Proxy
- Secret Manager

## **Module 08 - Securing Google Kubernetes Engine: Techniques and Best**

- Kubernetes Service Accounts
- Google Service Accounts
- GKE Security Best Practices
- GKE Monitoring and Logging

## **Module 09 - Protecting Against Distributed Denial-of-Service Attacks**

- DDoS Attack Mechanisms
- Google Cloud Mitigation Strategies
- Partner Security Products
- Cloud Armor

## **Module 10 - Content-Related Vulnerabilities: Techniques and Best**

- Ransomware Threats
- Data Misuse and Privacy Violations
- Cloud DLP API
- Sensitive Data Redaction

## **Module 11 - Monitoring, Logging, Auditing, and Scanning**

- Security Command Center
- Cloud Monitoring
- Cloud Logging
- Cloud Audit Logs
- Security Automation

## **Certification details**

CloudThat Course Completion Certificate will be awarded to all learners who complete the training.

## **FAQs**

**Who should attend this course?**

This course is designed for cloud security analysts, architects, engineers, and cybersecurity professionals working with Google Cloud.

**Is this course hands-on?**

Yes. The course includes multiple labs, security demonstrations, and monitoring exercises.

**What security services are covered?**

The course covers IAM, Cloud Armor, Cloud IDS, Secret Manager, Security Command Center, Cloud DLP API, and many other Google Cloud security services.

**Will Kubernetes security be covered?**

Yes. The course includes security best practices and monitoring techniques for Google Kubernetes Engine (GKE).

**Does the course include encryption and key management?**

Yes. CMEK, CSEK, Cloud HSM, and Cloud KMS concepts are covered extensively.

**What is the delivery format?**

The course is available in Instructor-Led Training (ILT) and On-Demand formats.

**Is prior security knowledge required?**

Yes. Foundational information security knowledge and cloud infrastructure familiarity are recommended.

**Will I receive a certificate?**

Yes. A CloudThat Course Completion Certificate will be awarded after successful completion of the training.