KOENIG
step forward

Security in Google Cloud Platform

This 2 day 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.

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 Outline

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.

- Module 1: Foundations of GCP Security
- Module 2: Cloud Identity
- Module 3: Identity and Access Management
- Module 4: Configuring Google Virtual Private Cloud for Isolation and Security
- Module 5: Monitoring, Logging, Auditing, and Scanning
- Module 6: Securing Compute Engine: techniques and best practices
- Module 7: Securing cloud data: techniques and best practices
- Module 8: Protecting against Distributed Denial of Service Attacks: techniques and best practices
- Module 9: Application Security: techniques and best practices
- Module 10: Content-related vulnerabilities: techniques and best practices