Vertex AI and Generative AI Security

Duration: 2 Days Course Code: GO8336 Delivery Method: Virtual Learning

Overview:

This course is designed to empower your organization to fully harness the transformative potential of Google's Vertex AI and generative AI (gen AI) technologies, with a strong emphasis on security.

Tailored for AI practitioners and security engineers, it provides targeted knowledge and hands-on skills to navigate and adopt AI safely and effectively. Participants will gain practical insights and develop a security-conscious approach, ensuring a secure and responsible integration of gen AI within their organization.
Products:
- Vertex AI
- Gemini
- Cloud IAM
- Cloud VPC
- Cloud KMS
- Cloud Operations
- Sensitive Data Protection

Updated August 2026

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

AI practitioners, security professionals, and cloud architects

Objectives:

- **After this course participants should be able to:**
- Review Google Cloud Security fundamentals.
- Establish a foundational understanding of Vertex AI.
- Enumerate the security concerns related to Vertex AI features and components.
- Control access with Identity Access Management.
- Simplify permission using organization hierarchies and policies.
- Use service accounts for least privileged access.
- Configure encryption at rest and in-transit.
- Encrypt data using customer-managed encryption keys.
- Protect sensitive data using the Data Loss Prevention service.
- Prevent exfiltration of data using VPC Service Controls.
- Architect systems with disaster recovery in mind.
- Deploy ML models using model endpoints.
- Secure model endpoints.
- Write to and analyze logs.
- Set up monitoring and alerting.
- Identify security risks specific to LLMs and gen AI applications.
- Understand methods for mitigating prompt hacking and injection attacks.
- Explore the fundamentals of securing generative AI models and applications.
- Introduce fundamentals of AI Safety.
- Implement best practices for testing model responses.
- Apply techniques for improving response security in gen AI applications.
- Understand RAG architecture and security implications.
- Implement best practices for grounding and securing data sources

in RAG systems.

Prerequisites:

- Fundamental knowledge of machine learning, in particular generative AI, and basic understanding of security on Google Cloud.

Testing and Certification

None

Follow-on-Courses:

None

Content:

Module 1: Introduction to Vertex AI Security Principles

- Google Cloud Security
- Vertex AI components
- Vertex AI Security concerns
- Lab: Vertex AI: Training and Serving a Custom Model

Module 2: Identity and Access Management (IAM) in Vertex AI

- Overview of IAM in Google Cloud
- Lab: Service Accounts and Roles: Fundamentals

Module 3: Data Security and Privacy

- Data encryption
- Protecting Sensitive Data
- VPC Service Controls
- Disaster recovery planning
- Lab: Getting Started with Cloud KMS
- Lab: Creating a De-identified Copy of Data in Cloud Storage

Module 4: Securing Vertex AI Endpoints and Model Deployment

- Network security
- Securing model endpoints
- Lab: Configuring Private Google Access and Cloud NAT

Module 5: Monitoring and Logging in Vertex AI

- Logging
- Monitoring

Module 6: Security Risks in Generative AI Applications

- Overview of gen AI security risks
- Overview of AI Safety
- Prompt security
- LLM safeguards
- Lab: Safeguarding with Vertex AI Gemini API
- Lab: Gen AI ; LLM Security for Developers

Module 7: Testing and Evaluating Generative AI Model Responses

- Testing generative AI model responses
- Evaluating model responses
- Fine-Tuning LLMs
- Lab: Measure Gen AI Performance with the Generative AI Evaluation Service
- Lab: Unit Testing Generative AI Applications

Module 8: Securing Retrieval-Augmented Generation (RAG) Systems

- Fundamentals of Retrieval-Augmented Generation
- Security in RAG systems
- Lab: Multimodal Retrieval Augmented Generation (RAG) Using the Vertex AI Gemini API
- Lab: Introduction to Function Calling with Gemini

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK