Vertex AI and Generative AI Security

Category: AI, Data & Analytics | **Vendor:** Google Cloud

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course 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.

About This Course

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.

Who Should Attend

AI practitioners, security professionals, and cloud architects

Prerequisites & Entry Requirements

General Prerequisites:

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Establish foundational knowledge of Vertex AI and its security challenges.
- Implement identity and access control measures to restrict access to Vertex AI resources.
- Configure encryption strategies and protect sensitive information.
- Enable logging, monitoring, and alerting for real-time security oversight of Vertex AI operations.
- Identify and mitigate unique security threats associated with generative AI.
- Apply testing techniques to validate and secure generative AI model responses.
- Implement best practices for securing data sources and responses within Retrieval-Augmented Generation (RAG) systems.
- Establish foundational knowledge of AI Safety.

Detailed Course Outline

Module 01 - Introduction to Vertex AI Security Principles

Topics

- Google Cloud Security
- Vertex AI components
- Vertex AI Security concerns

Objectives

- Review Google Cloud Security fundamentals.
- Establish a foundational understanding of Vertex AI.

- Enumerate the security concerns related to Vertex AI features and components.

Activities

- Lab: Vertex AI: Training and Serving a Custom Model

Module 02 - Identity and Access Management (IAM) in Vertex AI

Topics

- Overview of IAM in Google Cloud

Objectives

- Control access with Identity Access Management.
- Simplify permission using organization hierarchies and policies.
- Use service accounts for least privileged access.

Activities

- Lab: Service Accounts and Roles: Fundamentals

Module 03 - Data Security and Privacy

Topics

- Data encryption
- Protecting Sensitive Data
- VPC Service Controls
- Disaster recovery planning

Objectives

- 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.

Activities

- Lab: Getting Started with Cloud KMS
- Lab: Creating a De-identified Copy of Data in Cloud Storage

Module 04 - Securing Vertex AI Endpoints and model deployment

Topics

- Network security

- Securing model endpoints

Objectives

- Deploy ML models using model endpoints.

- Secure model endpoints.

Activities

- Lab: Configuring Private Google Access and Cloud NAT

Module 05 - Monitoring and logging in Vertex AI

Topics

- Logging

- Monitoring

Objectives

- Write to and analyze logs.

- Set up monitoring and alerting.

Module 06 - Security risks in generative AI applications

Topics

- Overview of gen AI security risks
- Overview of AI Safety
- Prompt security
- LLM safeguards

Objectives

- 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.

Activities

- Lab: Safeguarding with Vertex AI Gemini API
- Lab: Gen AI & LLM Security for Developers

Module 07 - Testing and evaluating generative AI model responses

Topics

- Testing generative AI model responses.

- Evaluating model responses.

- Fine-Tuning LLMs.

Objectives

- Implement best practices for testing model responses.

- Apply techniques for improving response security in gen AI applications

Activities

- Lab: Measure Gen AI Performance with the Generative AI Evaluation Service

- Lab: Unit Testing Generative AI Applications

Module 08 - Securing Retrieval-Augmented Generation (RAG) systems

Topics

- Fundamentals of Retrieval-Augmented Generation

- Security in RAG systems

Objectives

- Understand RAG architecture and security implications.

- Implement best practices for grounding and securing data sources in RAG systems.

Activities

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

Skills You Will Learn:

- Establish foundational knowledge of Vertex AI and its security challenges.
- Implement identity and access control measures to restrict access to Vertex AI resources.
- Configure encryption strategies and protect sensitive information.
- Enable logging, monitoring, and alerting for real-time security oversight of Vertex AI operations.
- Identify and mitigate unique security threats associated with generative AI.
- Apply testing techniques to validate and secure generative AI model responses.
- Implement best practices for securing data sources and responses within Retrieval-Augmented Generation (RAG) systems.
- Establish foundational knowledge of AI Safety.

Frequently Asked Questions

Q: What delivery options are available for Vertex AI and Generative AI Security?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Vertex AI and Generative AI Security course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Vertex AI and Generative AI Security training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Vertex AI and Generative AI Security?

Yes, we provide corporate training, dedicated training, and closed classes for Vertex AI and Generative AI Security. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Vertex AI and Generative AI Security, AI & Data Science, VAIGAS

Q: Why choose Nexus Human for Vertex AI and Generative AI Security?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Vertex AI and Generative AI Security training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 19/10/2026.