Model Armor: Securing AI Deployments

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

Duration: 1.00 hours (1 days) **0.8 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: vILT

Course Overview

This course reviews the essential security features of Model Armor and equips you to work with the service. You'll learn about the security risks associated with LLMs and how Model Armor protects your AI applications.

About This Course

This course reviews the essential security features of Model Armor and equips you to work with the service. You'll learn about the security risks associated with LLMs and how Model Armor protects your AI applications.

Prerequisites & Entry Requirements

General Prerequisites:

- Working knowledge of APIs
- Working knowledge of Google Cloud CLI
- Working knowledge of cloud security foundational principles
- Familiarity with the Google Cloud console

Learning Outcomes

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

Understand the essential security features and an overview of the Model Armor service.

Identify and explain the security risks associated with Large Language Models (LLMs).

Learn how to customize Model Armor by configuring floor settings, guard rails, and confidence levels.

Master the setup and usage of Model Armor, including API integration and handling flagged violations.

Apply Model Armor principles to real-world scenarios, including analyzing prompts, responses, and application code.

Detailed Course Outline

Course overview

What’s in it for me?

Model Armor overview

About Model Armor

LLM security risks

Customize Model Armor

About customization

Floor settings

Guard rails and confidence levels

Templates

Use Model Armor

About setup

API setup

Flagged violations

Put it all together

Prompts and responses

Application code

Course conclusion

What did I learn?

Frequently Asked Questions

Q: What delivery options are available for Model Armor: Securing AI Deployments?

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 1-day Model Armor: Securing AI Deployments course provides up to 0.8 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Model Armor: Securing AI Deployments training?

The training takes place over 1 day(s), with each day lasting approximately 1.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Model Armor: Securing AI Deployments?

Yes, we provide corporate training, dedicated training, and closed classes for Model Armor: Securing AI Deployments. 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: Model Armor: Securing AI Deployments, Google Cloud, vILT, Model Armor

---

Q: Why choose Nexus Human for Model Armor: Securing AI Deployments?

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 Model Armor: Securing AI Deployments 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.