Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810)

Category: AI, Data & Analytics | **Vendor:** Trivera Tech

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Dive into the rapidly evolving world of®Machine Learning Operations (MLOps) and AI Security®with our intensive 3-day boot camp. MLOps bridges the gap between data science and operation teams, delivering continuous collaboration and integration to drive the efficient production of AI models. Similarly, AI Security focuses on protecting AI systems from potential vulnerabilities, a critical skillset given the increasing reliance on AI in modern infrastructures. By mastering these skills, you'll be able to streamline machine learning projects and bolster security within your organization.

About This Course

Dive into the rapidly evolving world of Machine Learning Operations (MLOps) and AI Security with our intensive 3-day boot camp. MLOps bridges the gap between data science and operation teams, delivering continuous collaboration and integration to drive the efficient production of AI models. Similarly, AI Security focuses on protecting AI systems from potential vulnerabilities, a critical skillset given the increasing reliance on AI in modern infrastructures. By mastering these skills, you'll be able to streamline machine learning projects and bolster security within your organization.

Working in a hands-on workshop style environment guided by our AI security expert, you'll explore a wide range of topics and hands-on labs designed to provide a robust understanding of both MLOps and AI Security. Starting from an introduction to MLOps, you'll uncover the importance of this discipline, its distinction from DevOps and DataOps, and its lifecycle. You'll explore MLOps tools and techniques, including MLflow and Kubeflow, along with pipeline components and best practices. You will be able to set up an MLOps environment, automate ML workflows, monitor and manage models, and implement vital security measures in real-world situations. Lastly, you'll dive into the world of AI Security, exploring the AI threat landscape and best practices while applying basic security measures in a lab environment. The boot camp wraps up with advanced topics in AI Security, covering AI privacy, ethical considerations, adversarial attacks, and defenses.

Upon completion, you will have gained practical, hands-on skills in operationalizing and securing machine learning workflows, implementing best practices in model management, and understanding ethical considerations in AI Security. Our boot camp ensures that you will have the necessary knowledge to navigate MLOps and AI Security effectively, making your machine learning projects more efficient and secure.

Who Should Attend

The intermediate and beyond level course is a great fit for technical professionals eager to deepen their knowledge in machine learning and AI security. Roles such as Data Scientists, Machine Learning Engineers, IT Security Professionals, and DataOps Engineers would find significant value in this intensive, hands-on learning experience. This course is also suitable for technical leads and managers who oversee machine learning projects and need to understand both the operational and security aspects of AI systems.

Prerequisites & Entry Requirements

General Prerequisites:

Familiarity with basic machine learning concepts such as supervised and unsupervised learning, regression, classification, and neural networks will be beneficial.

-Experience with data preprocessing, feature engineering, and understanding of algorithms and data structures would be advantageous.

-Ideally, attendees should have practical experience with a programming language, preferably Python, given its prominence in machine learning and AI development. Those without programming background can follow along with the labs.

-Basic knowledge of cloud platforms like AWS, GCP, or Azure will be useful, especially regarding how they support machine learning operations and AI security.

-Prerequisites (courses)]]A general understanding of the software development process or lifecycle (SDLC), including stages like design, development, testing, and deployment, will be helpful as MLOps is a similar, but more specific, lifecycle.

Learning Outcomes

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

Throughout the course you'll learn how to:
-Gain a solid understanding of the Machine Learning Operations (MLOps) lifecycle, including its purpose, key elements, and how it differs from related fields like DevOps and DataOps.
-Develop practical skills in using key MLOps tools and techniques, such as setting up an MLOps environment using MLflow and Kubeflow, and working through a basic machine learning pipeline.
-Master the art of automating machine learning workflows to streamline and improve the efficiency of your machine learning projects.
-Familiarize yourself with the AI Security landscape, including threat identification and application of best practices for securing machine learning environments.
-Dive deep into advanced AI Security concepts, including understanding and implementing differential privacy in machine learning models and defending against adversarial attacks.
-Learn to balance technical implementation with ethical considerations, developing a well-rounded approach to AI Security that respects privacy concerns and adheres to ethical guidelines.

Detailed Course Outline

Day 1: Introduction to Machine Learning Operations (MLOps)

Introduction to MLOps

Understanding the need for MLOps

Differences between MLOps, DevOps, and DataOps

MLOps lifecycle overview

MLOps Tools and Techniques

Overview of MLOps tools (MLflow, Kubeflow, etc.)

MLOps pipeline components

MLOps best practices

Hands-on Lab: Setting Up an MLOps Environment using MLflow

Walking through a simple machine learning pipeline

Automating Machine Learning Workflows

The role of automation in MLOps

Continuous Integration and Continuous Deployment (CI/CD) in machine learning

Hands-on Lab: Automating ML workflows

Day 2: Advanced MLOps and Beginning AI Security

Model Monitoring and Management

Understanding model decay

Monitoring model performance in production

Model versioning and rollback

Hands-on Lab: Model Management

Implementing model monitoring with MLflow

Experimenting with model versioning and rollback

Introduction to AI Security

Understanding the need for AI Security

Overview of AI threat landscape

AI Security best practices

Hands-on Lab: Implementing basic security measures in a machine learning environment

Day 3: Advanced AI Security

AI Privacy and Ethical Considerations (2 hours)

Privacy risks in AI/ML applications

Understanding differential privacy

Ethical considerations in AI Security

Hands-on Lab: Implementing differential privacy in a machine learning model

AI Adversarial Attacks and Defenses

Understanding adversarial attacks

Techniques to defend against adversarial attacks

Hands-on Lab: Defending Against Adversarial Attacks

Implementing defense measures against sample adversarial attacks

Course Wrap-Up and Q&A

Additional Course Details

Nexus Humans Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810) training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810) course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810)?

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 3-day Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810) course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810) training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810)?

Yes, we provide corporate training, dedicated training, and closed classes for Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810). 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: AI; Machine Learning; MLOPs; DevOps, Security

---

Q: Why choose Nexus Human for Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810)?

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 Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (TTAI2810) 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 13/11/2026.