Machine Learning Operations (MLOPS) and AI Security

Duration: 03 Days

Course Overview

Gain practical skills in MLOps and AI Security, including pipeline setup, workflow automation, and threat identification

Dive into the rapidly evolving world of Machine Learning Operations (MLOps) and AI Security with our intensive 3-days training. 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.

Learning Objectives

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.

Machine Learning Operations (MLOPS) and AI Security

Who Should Attend

This intermediate to advanced 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.

Course Outline

Day 1: Introduction to Machine Learning Operations (MLOps)

1. Introduction to MLOps

- Understanding the need for MLOps
- Differences between MLOps, DevOps, and DataOps
- MLOps lifecycle overview

2. 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

3. 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

4. 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

5. 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

Machine Learning Operations (MLOPS) and AI Security

Day 3: Advanced AI Security

6. 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

7. 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

Pre-requisites

To ensure a smooth learning experience and maximize the benefits of attending this course, you should have the following prerequisite skills:

- 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.
- 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.