

**Tools for Monitoring AI/ML Training**

**Course Number:** PYTH-282WA  
**Duration:** 2 days

**Overview**

This Tools for Monitoring Artificial Intelligence and Machine Learning (AI/ML) training course teaches attendees how to implement AI/ML monitoring tools, select the right tools, and interpret the data the tools generate. Students also learn to detect and address model drift, monitor for data quality, privacy, and security, and ensure that the models meet their business objectives.

**Prerequisites**

Students must have basic knowledge of cloud architecture, machine learning, and data science pipelines.

**Materials**

All AI and ML training students receive comprehensive courseware.

**Software Needed on Each Student PC**

Detailed setup will be provided upon request.

**Objectives**

* Explain the importance of monitoring AI/ML models
* Identify the key metrics for monitoring AI/ML models
* Differentiate between monitoring for model performance and monitoring for application performance
* Implement tools and techniques for tracking data quality and detecting model drift
* Apply advanced AI/ML monitoring concepts, such as monitoring complex models at scale and mitigating adversarial attacks

**Outline**

* Introduction to Monitoring AI/ML Models
  + Importance of monitoring AI/ML models
  + Key metrics for monitoring AI/ML models
  + Monitoring for model performance vs. monitoring for application performance
  + Monitoring throughout the Data Science pipeline
* Monitoring Data Quality
  + Understanding data quality issues in AI/ML applications.
  + Tools and techniques for monitoring data quality.
  + How data quality issues affect model performance and strategies to manage this.
* Detecting and Addressing Model Drift
  + Understanding model drift
  + Techniques for detecting model drift and data drift
  + Tools for drift detection (e.g., AWS SageMaker Model Monitor, Seldon Alibi-Detect)
  + Strategies for addressing model drift
* Advanced Topics in AI/ML Monitoring
  + Monitoring complex models (e.g., deep learning models)
  + Monitoring at scale: big data considerations
  + Continuous monitoring and automated anomaly detection
* Monitoring for AI/ML Security
  + Understanding adversarial attacks on AI/ML models.
  + Importance of security monitoring in AI/ML.
  + Tools for monitoring and mitigating adversarial attacks.
* Privacy, Fairness, and Compliance Considerations
  + How privacy regulations impact AI/ML monitoring.
  + Tools and best practices for privacy-preserving AI/ML monitoring.
  + Case studies in AI/ML privacy and compliance.
  + Understanding model fairness and bias
  + Tools for fairness and bias monitoring (e.g., Fairlearn, Aequitas)
  + Case studies of fairness and bias monitoring
* Conclusion