Xerxez Solutions
Cooperate Training Road Map
On
DevSecOps/MLOps Full Stack Development Using MLFlow, Multi-Cloud System and End to End Security using GitHub Enterprises

This document provides the curriculum outline of the Knowledge, Skills and Abilities that a **Machine Learning Developer** and **DevOps/MLOps Administrator** can be expected to demonstrate.

Prerequisite:

- Fundamentals of Python Programming and Object-Oriented Technique.
- AWS Cli, Git/GitHub, DVC, Cookiecutter Template.
- Fundamental Knowledge of Django, Database, HTML/CSS.
- Fundamentals of Machine Learning Data Preprocessing, YAML, JSON.
- Basic AWS Cloud Service – EC2, EKS, ECS, EBS, S3 Bucket and RDS.
- Understanding of Visual Studio Framework.

Out Come:

After attending this training, the trainees will gain the below skills on Full Stack AI/ML Model Design, Development, Deploy & DevOps/MLOps Orchestration with end-to-end security using GitHub Enterprises.

- ML/MLOps Vs DevOps Framework using Multi-Cloud Architecture.
- Install/Configure Cookie Cutter Template and DVC (Data Tracking).
- Build Custom Environment for ML/MLOps model design and retraining using MLFlow.
- Manage DevOps/MLOps Lifecycle, Storage, CI/CD Pipeline using GitHub Action (Regression) and Jenkins (Deep Learning and NLP)
- Terraform for IaaS and Nagios for Continuous Monitoring.
- Model Deploying and scaling using Django Framework & PostgreSQL Database.
- Model Deployment using AWS ECS and AWS Fargate.
- Auditing and Troubleshooting Machine Learning Model.

- DevOps/MLOPs best Security Practices using GitHub Enterprise.

Local setup (Physical Mode)	Remote Lab Setup (Optional)	GitHub Enterprise Account
Laptop/Desktop with high-speed internet connection, Windows 10 and above	OS: Windows 10 and above	One Account
Memory: 4 GB RAM	Memory: 32 GB RAM	**Cloud Account**
CPU: 1 CPU Cores	CPU: 8 CPU Cores	Amazon Web Service (AWS)
Storage: 20 GB	Storage: 500 GB SSD	

Pilot Project

1. **Regression Technique**
2. **Deep Learning & Transfer Learning**
3. **NLP – Sentiment Analysis**
4. **Customer Data Segmentation - Clustering**

Topics Covered:

Introduction to MLOps using MLFlow:

- What is MLOps?
- Why we need MLOps and business impact?
- Machine learning industrialization challenges
- How does it relate to DevOps, AIOps, ModelOps, GitOps?

Introduction to MLOps stages:

- What are the various stages in ML lifecycle?
- Detailed MLOps Principles and stages
  - Versioning
  - Testing
  - Automation (CI/CD)
  - Reproducibility
  - Deployment
  - Monitoring

- MLOps Architectures:

  - Architectures \w Open-Source tools
  - Architectures \w cloud Native tools – Amazon Web Services
  - Comparison among cloud native tools

    - Cost-benefit approach of each architecture and MLOps maturity
- List of tools involved in each Stage (MLOps tool ecosystem).
- MLOps Maturity Model.
- Team ownership types in various stages of MLFlow.

Introduction to Model Management

- What is a Model Management?
- What are the various activities in Model Management?
- High-level overview of below Model Management tools
    - MLFlow
    - DVC

MLFlow Services

- What is MLFlow.
- Various components of MLFlow Services.
- Benefits of using MLFlow Services.

Hands-on:

1. Data Set from Kaggle is considered to demonstrate the real time Machine Learning Regression Model Design and Development. (Optional)
2. ML Model Retraining with an industry use case using CI/CD, ML Model using DVC.
3. Model Testing using Pytest and Linter Dependencies.

Introduction to Git/GitHub Enterprises:

- Overview of Git/GitHub Enterprises.
- Configure the Organization/ Repository/Team
- Understanding branching strategies, merge and pull request.
- Standard GIT branching strategies (development, feature, bug, release, UAT)
- Practicing important Git commands along with pilot project.
- End to End Secured Platform to Design, Develop and Deploy ML Model.
- Security:
    - Supply Chain – Dependency Graph, Advisory Database, Security Alerts & Update, Dependency Review.
    - Code – Secret Scanning and Code Scanning.
    - Branch Protection and Commit Signing.

Hands - on:

- Configure Organization, Team, and Repository.
- Building and Deploy ML pipeline in Github Action.

- Monitoring Model Performance using Nagios.

HashiCorp Terraform (Infrastructure as a Code)

- Terraform overview.
- Terraform Setup.
- Terraform On Cloud.
    - EC2 Instance Resources
    - S3 Bucket
    - RDS - PostgreSQL
    - Github - Repository
    - ECS
- Terraform Security Group
    - IAM Users and Working With Policies.
    - Token and Code Scanning.
- Challenges

Kubernetes/Docker Implementation (AWS ECS & EKS)

- Kubernetes overview
- Kubernetes Architecture
    - Nodes
    - Control Plane
    - API Server
- Kubernetes Resources
    - Pod
    - Deployment
    - Replica
    - Service
    - Volumes (PVC)
- Kubernetes Deployment Strategy
    - Monitoring
    - Liveness and Readiness Probes
- Labels and Selectors
- Docker Installation and Deployment.

Hands-on:

1. Kubernetes kubectl command practice.
2. Practice core concepts like AWS ECS, AWS Fargate and AWS EKS.
3. Use YAML construct for declarative commands.
4. Create and Deploy ML pipeline on Kubernetes and Containers.
5. Docker Compose File.

Amazon Web Service & Multi-Cloud Services

- EC2, S3 Bucket, RDS PostgreSQL
- EKS, ECS, Fargate,
- Identity Access Management.
- IAM Roles, Providers, SAML, OpenID, Web Identity.

Hands-on:

- Configure and Deploy Hybrid Cloud.
- Database Configuration PgAdmin tool.
- Zero Trust – Cloud Security Solution

Introduction to Django, PostgreSQL and Model Deployment using AWS.

- Why Django and PostgreSQL are important?
- What are the various types of front-end design related to machine learning model?
- Architecture of Django using Python Programming.
- User Data Storage using PostgreSQL Database.
- Model Deployment using ECS and Fargate Server

Hands-on:

- Building front end Graphical User Interface using Django, HTML/CSS
- Data Storage using PostgreSQL Database for future retraining of ML Model.

Introduction to Model Monitoring

- Why monitoring is important?
- What are the various types of monitoring related to machine learning model?
- Architecture of monitoring ecosystem in Nagios
- Various monitoring tools on Local Machine/Cloud Platform.

Hands-on:

- Building a drift monitoring system on Nagios.

CONTACT US

XERXEZ

Email : info@xerxez.in
WhatsApp: 9164315460
Website: www.xerxez.in