



CLOUD COMPUTING & DEVOPS

AWS . AZURE . GOOGLE CLOUD
KUBERNETES . TERRAFORM
JENKINS . DEVSECOPS . OBSIDIAN

DURATION

250–350 Hours

SPAN

5–7 Months

MODULES

17

MODE

**Classroom •
Online • Hybrid**

01 COURSE OVERVIEW

A master programme covering three cloud platforms and the DevOps toolchain that runs on them. Learners begin with Linux administration, networking and Git, then work through AWS, Azure and Google Cloud Platform, containers and Kubernetes, infrastructure as code with Terraform, CI/CD with Jenkins, DevSecOps, monitoring, configuration management, cloud security and multi-cloud architecture.

Module 12 is delivered in its expanded twelve-session form; the session-by-session breakdown is set out in the appendix to this handout. The programme closes with 50 hours of industry projects.

WHO IT IS FOR

System and network administrators moving to cloud
Developers taking on deployment and pipeline work
Support engineers targeting DevOps roles
Graduates with networking and Linux fundamentals

PREREQUISITES

Basic knowledge of networking, Linux and programming fundamentals.

02 LEARNING OUTCOMES

01 Administer Linux servers and automate routine work with shell scripts.

03 Build and operate workloads across AWS, Azure and Google Cloud.

05 Provision infrastructure declaratively with Terraform modules and state.

07 Embed security scanning, secrets management and policy into pipelines.

09 Plan cloud migration, backup, disaster recovery and cost governance.

02 Design cloud networks with VPCs, subnets, DNS and load balancing.

04 Containerise applications and run them on Kubernetes with Helm.

06 Build CI/CD pipelines in Jenkins and GitHub Actions.

08 Monitor clusters and applications with Prometheus, Grafana and the ELK stack.

03 MODULE STRUCTURE

17 MODULES

01 INTRODUCTION TO CLOUD COMPUTING

10 HOURS

Introduction to Cloud Computing

Cloud Service Models (IaaS, PaaS, SaaS)

Virtualization vs Containerization

Shared Responsibility Model

Cloud Cost Optimization

Evolution of Cloud Technology

Deployment Models (Public, Private, Hybrid, Multi-Cloud)

Cloud Architecture

Cloud Security Fundamentals

Cloud Use Cases

PRACTICAL

CREATE FREE TIER CLOUD ACCOUNTS

CLOUD RESOURCE MANAGEMENT

INTRODUCTION TO AWS, AZURE, AND GCP CONSOLES

02 LINUX ADMINISTRATION FOR CLOUD

20 HOURS

Linux Installation

Users & Groups

Package Management

Networking Commands

Cron Jobs

System Monitoring

Linux File System

File Permissions

Process Management

Shell Scripting

SSH & Remote Access

PRACTICAL

CONFIGURE LINUX SERVERS

WRITE BASH SCRIPTS

MANAGE REMOTE SERVERS

03 NETWORKING FOR CLOUD ENGINEERS

20 HOURS

OSI & TCP/IP Models

Subnetting

DNS

NAT

Firewalls

CDN Basics

IP Addressing

Routing & Switching

DHCP

VPN

Load Balancing

PRACTICAL

NETWORK CONFIGURATION

TROUBLESHOOTING

VPC NETWORK DESIGN

04 GIT & GITHUB

15 HOURS

Version Control

Repository Management

Merging

Pull Requests

Collaboration Workflows

Git Installation

Branching

Rebasing

GitHub Actions

Git Best Practices

PRACTICAL

CREATE GIT REPOSITORIES

TEAM COLLABORATION

CI WITH GITHUB ACTIONS

05 AMAZON WEB SERVICES (AWS)

45 HOURS

AWS Global Infrastructure

EC2

EBS

VPC

Elastic Load Balancer (ELB)

CloudWatch

AWS Lambda

DynamoDB

SQS

CloudFormation

IAM

S3

EFS

Route 53

Auto Scaling

CloudTrail

RDS

SNS

API Gateway

Cost Management

PRACTICAL

LAUNCH EC2 INSTANCES

HOST STATIC WEBSITES ON S3

CONFIGURE VPC

DEPLOY WEB APPLICATIONS

06 MICROSOFT AZURE

35 HOURS

Azure Portal

Azure Virtual Network

Azure App Services

Azure SQL Database

Azure Active Directory

Azure Security Center

Azure Virtual Machines

Azure Storage

Azure Functions

Azure Kubernetes Service (AKS)

Azure Monitor

PRACTICAL

DEPLOY VIRTUAL MACHINES

BUILD AZURE WEB APPS

CONFIGURE AZURE NETWORKING

07 GOOGLE CLOUD PLATFORM (GCP)

30 HOURS

GCP Architecture

Cloud Storage

IAM

Cloud Functions

Kubernetes Engine (GKE)

Monitoring & Logging

Compute Engine

Cloud SQL

VPC

Cloud Run

PRACTICAL

DEPLOY APPLICATIONS ON GCP

CONFIGURE CLOUD STORAGE

MANAGE COMPUTE RESOURCES

08 DOCKER

25 HOURS

Containerization

Docker Images

Dockerfile

Docker Volumes

Multi-stage Builds

Docker Hub

Docker Architecture

Docker Containers

Docker Compose

Docker Networking

Docker Registry

PRACTICAL

BUILD DOCKER IMAGES

CONTAINERIZE APPLICATIONS

DOCKER COMPOSE PROJECTS

09 KUBERNETES

35 HOURS

Kubernetes Architecture

ReplicaSets

Services

Secrets

StatefulSets

Ingress

Horizontal Pod Autoscaler

Pods

Deployments

ConfigMaps

Persistent Volumes

DaemonSets

Helm

Kubernetes Security

PRACTICAL

DEPLOY APPLICATIONS

SCALE APPLICATIONS

KUBERNETES CLUSTER MANAGEMENT

10 INFRASTRUCTURE AS CODE (TERRAFORM)

20 HOURS

Infrastructure as Code (IaC)

Providers

Variables

Modules

Remote Backend

Terraform Cloud

Terraform Installation

Resources

Outputs

State Management

Workspaces

PRACTICAL

PROVISION AWS INFRASTRUCTURE

DEPLOY MULTI-TIER ARCHITECTURE

11 JENKINS & CI/CD

30 HOURS

Continuous Integration (CI)

Continuous Deployment

Jenkins Pipelines

Pipeline as Code

Artifact Management

Git Integration

Continuous Delivery (CD)

Jenkins Installation

Declarative Pipelines

Build Automation

Notifications

PRACTICAL

BUILD CI/CD PIPELINES

AUTOMATE APPLICATION DEPLOYMENT

12 DEVSECOPS

25 HOURS

DevSecOps Fundamentals

Vulnerability Assessment

Dependency Scanning

Dynamic Application Security Testing (DAST)

Kubernetes Security

Compliance (ISO 27001, SOC 2, PCI DSS)

Secure SDLC

Secrets Management

Static Application Security Testing (SAST)

Container Security

Cloud Security Best Practices

TOOLS

SONARQUBE

TRIVY

OWASP ZAP

SNYK

HASHICORP VAULT

PRACTICAL

SECURE CI/CD PIPELINES

CONTAINER VULNERABILITY SCANNING

13 MONITORING & LOGGING

20 HOURS

Monitoring Concepts

Metrics

Dashboards

Logging Best Practices

Alerts

Application Performance Monitoring (APM)

TOOLS

PROMETHEUS

GRAFANA

ELK STACK (ELASTICSEARCH, LOGSTASH, KIBANA)

LOKI

FLUENTD

PRACTICAL

MONITOR KUBERNETES CLUSTERS

BUILD GRAFANA DASHBOARDS

14 AUTOMATION & CONFIGURATION MANAGEMENT

20 HOURS

Automation Fundamentals

Playbooks

Inventory Management

Server Provisioning

Ansible Architecture

Roles

Configuration Management

PRACTICAL

AUTOMATE SERVER CONFIGURATION

MULTI-SERVER DEPLOYMENT

15 CLOUD SECURITY & GOVERNANCE

20 HOURS

Identity & Access Management (IAM)

Key Management

Network Security

Governance Policies

High Availability

Encryption at Rest & In Transit

Security Groups

Cloud Compliance

Backup & Disaster Recovery

Cost Governance

PRACTICAL

SECURE CLOUD INFRASTRUCTURE

IMPLEMENT BACKUP STRATEGIES

16 MULTI-CLOUD & HYBRID CLOUD

15 HOURS

Multi-Cloud Strategy

Cloud Migration

Cloud Cost Optimization

Hybrid Cloud Architecture

Disaster Recovery

Cross-Cloud Networking

PRACTICAL

DEPLOY MULTI-CLOUD APPLICATIONS

17 CAPSTONE PROJECTS

50 HOURS

INDUSTRY PROJECTS

DEPLOY A THREE-TIER WEB APPLICATION ON AWS

CI/CD PIPELINE WITH JENKINS, DOCKER, AND KUBERNETES

INFRASTRUCTURE PROVISIONING WITH TERRAFORM

MULTI-CLOUD DEPLOYMENT (AWS + AZURE + GCP)

KUBERNETES CLUSTER MONITORING WITH PROMETHEUS & GRAFANA

SECURE DEVSECOPS PIPELINE

AUTO-SCALING CLOUD INFRASTRUCTURE

CLOUD MIGRATION PROJECT

CONTAINERIZED MICROSERVICES DEPLOYMENT

SERVERLESS APPLICATION USING AWS LAMBDA OR AZURE FUNCTIONS

04 APPENDIX — DEVSECOPS (ADVANCED)

25 HOURS · 12
SESSIONS

Enable learners to integrate security into every phase of the Software Development Life Cycle (SDLC) by implementing DevSecOps practices, securing CI/CD pipelines, containers, Kubernetes environments, and cloud infrastructure while ensuring compliance with industry standards.

01 INTRODUCTION TO DEVSECOPS

3 HOURS

Introduction to DevOps vs DevSecOps

Evolution of DevSecOps

Shift Left Security

DevSecOps Lifecycle

Roles and Responsibilities

Why Security in DevOps?

DevSecOps Principles

Shared Responsibility Model

Security Culture in Organizations

DevSecOps Pipeline Overview

PRACTICAL

SET UP A SECURE DEVOPS ENVIRONMENT

INSTALL GIT, JENKINS, DOCKER, AND SONARQUBE

BUILD A SIMPLE DEVSECOPS PIPELINE

02 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SECURE SDLC)

3 HOURS

SDLC Overview

Security Requirements Gathering

Threat Modeling

Code Review Best Practices

Risk Assessment

Secure SDLC Phases

Secure Architecture Design

Secure Coding Standards

Security Testing Throughout the SDLC

OWASP Secure Coding Practices

PRACTICAL

CREATE A SECURE SDLC WORKFLOW

PERFORM THREAT MODELING USING MICROSOFT THREAT MODELING TOOL

03 VULNERABILITY ASSESSMENT & RISK MANAGEMENT

2 HOURS

Vulnerability Assessment Fundamentals

CVSS Scoring

Common Vulnerabilities

Vulnerability Remediation Process

Risk Assessment Methodology

Vulnerability Classification

Security Baselines

TOOLS

OPENVAS / GREENBONE

NESSUS ESSENTIALS

NMAP

NIKTO

PRACTICAL

SCAN A LINUX SERVER

ANALYZE VULNERABILITIES

PREPARE A REMEDIATION REPORT

04 SECRETS MANAGEMENT

2 HOURS

What are Secrets?

SSH Keys

Certificates

Secret Rotation

Least Privilege Principle

API Keys

Password Management

Environment Variables

Secure Storage

TOOLS

HASHICORP VAULT

AWS SECRETS MANAGER

AZURE KEY VAULT

KUBERNETES SECRETS

PRACTICAL

CONFIGURE HASHICORP VAULT

STORE AND RETRIEVE APPLICATION SECRETS

INTEGRATE VAULT WITH JENKINS

05 DEPENDENCY & SOFTWARE COMPOSITION ANALYSIS (SCA)

2 HOURS

Third-Party Library Risks

Dependency Management

License Compliance

Package Security

Software Supply Chain Security

Software Bill of Materials (SBOM)

CVE Databases

TOOLS

OWASP DEPENDENCY-CHECK

SNYK

TRIVY

GITHUB DEPENDABOT

PRACTICAL

SCAN APPLICATION DEPENDENCIES

GENERATE VULNERABILITY REPORTS

UPDATE VULNERABLE PACKAGES

06 STATIC APPLICATION SECURITY TESTING (SAST)

2 HOURS

Introduction to SAST

Common Coding Vulnerabilities

CWE Overview

Secure Coding Practices

Secure Code Analysis

OWASP Top 10

Code Quality Metrics

TOOLS

SONARQUBE

SEMGREP

CHECKMARX (OVERVIEW)

PRACTICAL

SCAN JAVA/PYTHON APPLICATIONS

IDENTIFY SECURITY FLAWS

FIX CODING VULNERABILITIES

07 DYNAMIC APPLICATION SECURITY TESTING (DAST)

2 HOURS

DAST Concepts

Web Application Vulnerabilities

Session Management Testing

OWASP Top 10 Testing

Runtime Security Testing

Authentication Testing

API Security Testing

TOOLS

OWASP ZAP

BURP SUITE COMMUNITY

NIKTO

PRACTICAL

SCAN A WEB APPLICATION

IDENTIFY VULNERABILITIES

GENERATE SECURITY REPORTS

08 CONTAINER SECURITY

2 HOURS

Docker Security

Image Signing

Container Isolation

Docker Bench for Security

Secure Docker Images

Image Scanning

Runtime Security

CIS Docker Benchmark

TOOLS

DOCKER

TRIVY

DOCKER SCOUT

CLAIR

PRACTICAL

SCAN DOCKER IMAGES

HARDEN DOCKERFILES

REMOVE VULNERABLE PACKAGES

09 KUBERNETES SECURITY

2 HOURS

Kubernetes Security Architecture

Network Policies

Admission Controllers

Namespace Isolation

Image Policies

RBAC

Pod Security Standards

Secret Management

Secure Ingress

Runtime Protection

TOOLS

KUBE-BENCH

KUBE-HUNTER

FALCO

KYVERNO

PRACTICAL

SECURE A KUBERNETES CLUSTER

CONFIGURE RBAC

IMPLEMENT NETWORK POLICIES

SCAN KUBERNETES SECURITY

10 CLOUD SECURITY BEST PRACTICES

2 HOURS

Cloud Shared Responsibility Model

Multi-Factor Authentication (MFA)

Key Management

Network Security

Backup & Disaster Recovery

Identity & Access Management (IAM)

Encryption at Rest & In Transit

Security Groups

Logging & Monitoring

Zero Trust Architecture

CLOUD PLATFORMS

AWS

MICROSOFT AZURE

GOOGLE CLOUD PLATFORM (GCP)

PRACTICAL

CONFIGURE IAM POLICIES

ENABLE CLOUD LOGGING

SECURE CLOUD STORAGE

IMPLEMENT MFA

11 COMPLIANCE & GOVERNANCE

2 HOURS

Security Governance

Compliance Frameworks

SOC 2

GDPR (Overview)

Audit Readiness

Risk Management

ISO/IEC 27001

PCI DSS

HIPAA (Overview)

Security Documentation

PRACTICAL

COMPLIANCE CHECKLIST CREATION

SECURITY POLICY DOCUMENTATION

RISK REGISTER PREPARATION

12 DEVSECOPS CI/CD INTEGRATION

1 HOURS

Security Gates in CI/CD

Policy as Code

Security Monitoring

Automated Security Testing

Continuous Compliance

Incident Response Automation

PRACTICAL

BUILD A SECURE JENKINS PIPELINE

INTEGRATE SONARQUBE, TRIVY, AND OWASP ZAP INTO CI/CD

HANDS-ON LABS

SECURE GIT REPOSITORY CONFIGURATION

JENKINS PIPELINE WITH SECURITY CHECKS

SONARQUBE CODE ANALYSIS

TRIVY CONTAINER IMAGE SCANNING

OWASP ZAP WEB APPLICATION SECURITY TESTING

HASHICORP VAULT SECRETS MANAGEMENT

KUBERNETES SECURITY HARDENING

CLOUD IAM POLICY CONFIGURATION

AUTOMATED DEPENDENCY SCANNING

COMPLIANCE AUDIT PREPARATION

MINI PROJECTS

BUILD A SECURE CI/CD PIPELINE USING JENKINS, GITHUB, SONARQUBE, TRIVY, AND DOCKER.

SECURE A KUBERNETES APPLICATION USING RBAC, NETWORK POLICIES, AND FALCO.

IMPLEMENT CENTRALIZED SECRETS MANAGEMENT WITH HASHICORP VAULT.

PERFORM VULNERABILITY ASSESSMENT AND REMEDIATION FOR A WEB APPLICATION.

CONDUCT A CLOUD SECURITY AUDIT FOR AWS OR AZURE RESOURCES.

05 TOOLS & TECHNOLOGIES COVERED

CLOUD PLATFORMS

AMAZON WEB SERVICES (AWS)

MICROSOFT AZURE

GOOGLE CLOUD PLATFORM (GCP)

CONTAINERS & ORCHESTRATION

DOCKER

KUBERNETES

HELM

DEVOPS & AUTOMATION

GIT

GITHUB

GITHUB ACTIONS

JENKINS

TERRAFORM

ANSIBLE

MONITORING & LOGGING

PROMETHEUS

GRAFANA

ELK STACK

LOKI

FLUENTD

SECURITY TOOLS

SONARQUBE

TRIVY

SNYK

OWASP ZAP

HASHICORP VAULT

SUPPORTING TECHNOLOGIES

LINUX

BASH SCRIPTING

YAML

JSON

SSH

REST APIS

06 ASSESSMENT & CERTIFICATION

Module assignments and labs	25%
Mini projects	20%
Internal assessments	15%
Capstone project and review	40%

CERTIFICATION

Learners who complete all modules, submit the capstone project and clear the final review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio and GitHub profile, and interview preparation is included in the final week.

07 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

CLOUD ENGINEER

DEVOPS ENGINEER

SITE RELIABILITY ENGINEER

KUBERNETES ADMINISTRATOR

CLOUD ARCHITECT

DEVSECOPS ENGINEER

PLATFORM ENGINEER

CLOUD SUPPORT ENGINEER

CALL US

+91 73051 33996

EMAIL US

apply@kaizeninfinities.com

VISIT OUR WEBSITE

www.kaizeninfinities.com