



DEVSECOPS

SHIFT LEFT . SECURE SDLC .
SAST . DAST . SCA . SECRET
TAINER . KUBERNETES . CLO

DURATION

25 Hours

LEVEL

Advanced

MODULES

8

MODE

**Classroom ·
Online · Hybrid**

01 COURSE OVERVIEW

A security-in-pipeline course: threat modelling, scanning, secrets management and compliance evidence. Security controls are added to a working pipeline stage by stage — dependency scanning, static and dynamic analysis, image scanning, policy as code and secrets management — with each control tuned to keep build times workable.

The course follows the twelve-session structure delivered inside the Cloud & DevOps master programme.

WHO IT IS FOR

DevOps and platform engineers

Security engineers joining delivery teams

Developers responsible for secure code

Compliance and audit staff

PREREQUISITES

Git, Docker, one CI tool and basic Linux security knowledge.

02 LEARNING OUTCOMES

01 Model threats before code is written.

03 Scan and harden container images.

05 Secure a Kubernetes cluster with RBAC and policies.

07 Assemble audit evidence for ISO 27001, SOC 2 and PCI DSS.

02 Gate builds on dependency and code scanning.

04 Manage secrets centrally with rotation.

06 Apply cloud IAM and logging baselines.

03 MODULE STRUCTURE

8 MODULES

01 DEVSECOPS FOUNDATIONS

DevOps vs DevSecOps

Shared responsibility

Pipeline overview

Shift-left security

Security culture

LAB

SECURE TOOLCHAIN SETUP

02 SECURE SDLC

Requirements

Threat modelling

Code review

Secure design

Secure coding standards

Risk assessment

LAB

THREAT MODEL

03 VULNERABILITY MANAGEMENT

Assessment methodology

CVSS

Classification

Baselines

Remediation workflow

TOOLS

OPENVAS

NMAP

NIKTO

04 SECRETS MANAGEMENT

Secret types

Storage

Rotation

Least privilege

Pipeline injection

TOOLS

HASHICORP VAULT

AWS SECRETS MANAGER

AZURE KEY VAULT

05 DEPENDENCY AND SUPPLY CHAIN

Third-party risk

SBOM

License compliance

CVE feeds

Pinning and updates

TOOLS

SNYK

TRIVY

DEPENDABOT

06 SAST AND DAST

Static analysis

OWASP Top 10

CWE

Runtime scanning

API testing

Triage of findings

TOOLS

SONARQUBE

SEMGREP

OWASP ZAP

07 CONTAINER AND KUBERNETES SECURITY

Image hardening

Runtime security

Network policies

Signing

RBAC

Admission control

TOOLS

TRIVY

KUBE-BENCH

FALCO

KYVERNO

08 CLOUD, COMPLIANCE AND INTEGRATION

IAM baselines

Logging

ISO 27001

PCI DSS

Encryption and keys

Zero trust

SOC 2

Security gates in CI/CD

PROJECT

SECURE PIPELINE WITH FULL EVIDENCE PACK

04 ASSESSMENT & CERTIFICATION

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

CERTIFICATION

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

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

DEVSECOPS ENGINEER

APPLICATION SECURITY ENGINEER

CLOUD SECURITY ENGINEER

COMPLIANCE ENGINEER

PLATFORM SECURITY LEAD

CALL US

+91 73051 33996

EMAIL US

apply@kaizeninfinities.com

VISIT OUR WEBSITE

www.kaizeninfinities.com