Kore Infotech
Intelligent IT Solutions
Passionate People

DevSec Ops Course

The DevSecOps course is designed to help IT professionals integrate robust security practices into the DevOps lifecycle. Participants will learn how to embed security controls, automation, and compliance into continuous integration and continuous delivery (CI/CD) pipelines.
The course covers key DevOps and DevSecOps principles, identity and access management (IAM), application and operational security, secure SDLC, and container security with Docker and Kubernetes. Learners will also explore governance, risk management, and compliance (GRC) frameworks, along with hands-on demonstrations of secure cloud and container environments. By the end of the course, participants will be able to align speed, agility, and innovation with enterprise-grade security in modern DevOps workflows.

Who Should Attend This Course:

This course is ideal for DevOps engineers, security professionals, system administrators, software developers, cloud engineers, and IT managers who want to strengthen their understanding of integrating security seamlessly within DevOps processes.

Pre-Requisites:

- Basic understanding of **DevOps concepts** and software development life cycles.
- Familiarity with **cloud platforms** (AWS, Azure, or GCP) and **container technologies** (Docker, Kubernetes) is recommended.
- Prior exposure to **networking or system administration** will be helpful but not mandatory.

Course Duration:

This course will be conducted over a period of 3 Days (9.30 am to 5.30 pm)

Objectives:

1. Understand DevOps and DevSecOps fundamentals — their principles, goals, values, and the importance of integrating security early in the pipeline.
2. Apply security practices across the CI/CD pipeline, including secure SDLC, threat modeling, and automated security testing.
3. Implement identity and access management (IAM), encryption, and policy management for secure infrastructure and applications.
4. Enhance operational security through logging, monitoring, incident response, and threat intelligence integration.
5. Secure containerized and cloud environments, including Docker, Kubernetes, and AWS-based deployments.
6. Align DevSecOps initiatives with GRC frameworks to ensure compliance, risk management, and continuous audit readiness.

Kore Infotech
Intelligent IT Solutions
Passionate People

Course Content

1. **DevOps Foundation Review**
   - 1.1. What is DevOps?
   - 1.2. DevOps Goals
   - 1.3. DevOps Values
   - 1.4. DevOps Stakeholders

2. **Why DevSecOps?**
   - 2.1. Key Terms and Concepts
   - 2.2. Why DevSecOps is important
   - 2.3. Key Principles of DevSecOps

3. **Strategic Considerations**
   - 3.1. Key Terms and Concepts
   - 3.2. How Much Security is Enough?
   - 3.3. Threat Modelling
   - 3.4. Risk Management in a High-velocity World

4. **Identity & Access Management (IAM)**
   - 4.1. IAM Basic Concepts
   - 4.2. Why IAM is Important
   - 4.3. Implementation Guidance
   - 4.4. Automation Opportunities

5. **Application Security**
   - 5.1. Application Security Testing (AST)
   - 5.2. Testing Techniques
   - 5.3. Issue Management Integration
   - 5.4. Leveraging Automation

6. **Operational Security**
   - 6.1. Key Terms and Concepts
   - 6.2. Basic Security Hygiene Practices
   - 6.3. Role of Operations Management

7. **Logging, Monitoring and Response**
   - 7.1. Key Terms and Concepts
   - 7.2. Setting Up Log Management
   - 7.3. Incident Response and Forensics
   - 7.4. Threat Intelligence and Information Sharing

8. **Overview of Information Security**
   - 8.1. Ethical Hacking vs Cyber Security vs Information Security
   - 8.2. Policy Management
   - 8.3. Password Management
   - 8.4. Encryption
   - 8.5. Standards, Best Practices, and Regulations
   - 8.6. Threat Modelling and Risk Management
   - 8.7. Social Engineering
   - 8.8. Phishing/Spear Phishing/Whaling

9. **Understanding Application & Infrastructure Security**
   - 9.1. DevOps, Cloud, and Their Impact on Traditional Security Architecture
   - 9.2. Traditional Software Development Security
   - 9.3. Securing the DevOps Pipeline

10. **Addressing 2018 OWASP Security Guidelines as Part of the CI/CD** Pipeline
    - 10.1. What is Secure SDLC
    - 10.2. Secure SDLC Activities and Security Gates
    - 10.3. SaaS Security Concepts
    - 10.4. PaaS Security Concepts
    - 10.5. IaaS Security Concepts

11. **Securing Container Management and Orchestration Activities**
    - 11.1. Docker Container Security Demonstration
    - 11.2. Docker Architecture
    - 11.3. Docker Hardening
    - 11.4. AWS EC2 Container Services
    - 11.5. Securing Kubernetes
    - 11.6. Kubernetes Security Demonstration
    - 11.7. Secure Container Management and Orchestration Module

12. **Governance, Risk Management, Compliance & Audit**
    - 12.1. What is GRC?
    - 12.2. Why care about GRC?
    - 12.3. Policy as Code
    - 12.4. Audit & Compliance
    - 12.5. 3 Myths of Separation of Duties