MASET

APPROVED LEARNING & TRAINING INSTITUTION

DevOps Foundation

Learning Mode:
Online

Duration:
3 Days Training + Post Class Coaching

This course is specifically designed to provide participants with:

- DevOps objectives and vocabulary
- Benefits to the business Concepts and practices — including its relationship to Agile, Lean IT and IT Service Management (ITSM)
- Improved workflows
- Improved communication and feedback loops
- Reliance on automation
- Applying DevOps in an enterprise environment
- Critical success factors and key performance indicators
- Real-life examples and results

Trainer:

SHAILENDRASINGH NAIYYAR
25 years industry experience

A certified ITIL 4 Master and accredited trainer for EXIN® and PEOPLECERT®, Shailendrasingh Naiyyar is a ServiceNow Platform Lead at Syngenta Services with a strong foundation in agile service management across Telecom, Finance, Health Informatics, and Digital Agronomy domains. With a Master's in Computer Applications (1999), he specializes in service design, ITSM, process transformation, DevOps leadership, and digital enterprise enablement.

Accredited by:

PeopleCert
All talents, certified.

Course Overview

SUMMARY
This course covers the basics of DevOps, a method that connects development and operations to improve software delivery. You'll learn how to boost teamwork, automate tasks, and use CI/CD pipelines to deliver better software faster. Great for professionals who want to work more efficiently and keep up with changing customer needs.

Course Content

MODULE 1 – Realizing DevSecOps outcomes
MODULE 2 – Defining the Cyber Threat Landscape(CTL)
MODULE 3 – Building a responsive DevSecOps model
MODULE 4 – Integrating DevSecOps stakeholders
MODULE 5 – Establishing DevSecOps best practices
MODULE 6 – Best practices to get started
MODULE 7 – DevOps pipelines and continuous compliance
MODULE 8 – Learning using outcomes

This course is specifically designed to provide participants with:

- Agile
- API
- Architecture
- Artifact management
- Authentication
- Authorization
- Access management
- Advice process
- Binary Instrumentation
- Business continuity plan
- Business transformation
- CALMS
- CIA triad
- CICD pipeline
- Chaos Engineering
- Container security
- Continuous compliance
- Continuous security
- Cross-skilling
- Cyberthreat Landscape
- DevSecOps
- DIE
- DREAD
- Dynamic Application Security Testing (DAST)
- Cooperation
- Erickson
- Fuzzing
- Governance, Risk management and Compliance (GRC) platform
- Identity
- Identity and Access Management (IAM)
- Incident response
- Interactive Application Security Testing (IAST)
- Issue management
- Laloux
- Log management
- Mean Time to Change (MTTC)
- Mean Time to Detect (MTTD)
- Mean Time to Recover (MTTR)
- Multi-factor authentication
- OCTAVE
- Ops management
- Patch
- Patch management
- Penetration testing
- Policy as code (PaC)
- Privileged access management
- RACI
- Real Time Application Self-Protection (RASP)
- Resilience
- Retrospective
- Risk management
- Roles
- Role-based access control
- Safety culture
- Secrets management
- Security as code (SaC)
- Security Information and Event Management (SIEM)
- Separation of Duties (SOD)
- Shared vision and objectives
- Shift left
- Site Reliability Engineering (SRE)
- Software Composition Analysis (SCA)
- Stakeholder Modeling
- Static Application Security Testing (SAST)
- STRIDE
- System of record
- Supply Chain
- Telemetry
- The Three Ways
- Threat
- Threat modelling
- Threat intelligence
- Value Stream
- Vulnerability
- Vulnerability management
- Vulnerability scans
- Westrum