Course Design and Outline

Learning Program	Duration
DEVSECOPS	3 days

Prerequisites

The DevOps Foundation certification is a prerequisite for DevSecOps Engineering to ensure participants are aligned with the baseline DevOps definitions and principles

Learning Program Overview

Course name and description	**DEVSECOPS**
Course learning objectives	The learning objectives include a practical understanding of: • The purpose, benefits, concepts, and vocabulary of DevSecOps • How DevOps security practices differ from other security approaches • Business-driven security strategies • Understanding and applying data and security sciences • The use and benefits of Red and Blue Teams • Integrating security into Continuous Delivery workflows • How DevSecOps roles fit with a DevOps culture and organization

Program Outline

Program Name	DEVSECOPS	Est. time
Instructional Strategy	• In this course, you will learn how to • Explain the purpose, benefits, concepts and vocabulary of DevSecOps • Differentiate DevOps security practices from other security approaches • Focus on Business-driven security strategies • Apply data and security sciences • Benefit from Security Testing with Red and Blue Teams • Integrate security into Continuous Delivery workflows • Integrate DevSecOps roles with a DevOps culture and organization	
Lesson	**Topics**	
DevSecOps Approach, Framework and Toolkit	• DevOps fundamentals • Why a traditional security approach doesn't work	1 Hrs.
	• What is DevSecOps? • DevSecOps approach	1 Hrs.
	• DevSecOps framework • DevSecOps toolkit • The Jenkins approach	1 Hrs.
	• Lab: Application Development Pipeline	1 Hrs.
Automated Application Security Testing	• OWASP Top 10 • Secure Software Development Lifecycle • Application Security Layer Testing Tools • Lab: Integrate Application Security Test to Pipeline	2.5 Hrs.
Infrastructure as Code and Unit Tests	• Infrastructure as Code • Unit Tests • Lab: InSpec	1.5 Hrs.
Cloud Security AWS EC2	• Infrastructure as Code • Unit Tests • Lab: InSpec	2.5 hour
Continuous Compliance Continuous Compliance Framework	• Policy as code • Audit as code • Lab: Cloud Compliance • Lab: Discover Secrets • Demo: Policy as code in Azure	3.5 hours
Security flow in Jenkins Deployment Pipeline	• Static Analysis • Security Unit Tests	2 hours

	• IDE Integration • Code Review • Dynamic Analysis • Result verification • Dynamic Testing • WaF / RASP • Risk Analysis Tests Review • Demo: Fortify on Demand & Fortify WebInspect	
Containers	• Concept of containers • Docker • Security Issues of containers • Orchestration • Container security solutions • Integration to CI / CD pipeline • Lab: Container security	2.5 hours
Serverless	• Concept of serverless • AWS Lambda, Azure Cloud Functions, Google Cloud Functions • Serverless application architecture • Security implications • Lab: Deploy serverless application to cloud using CI / CD pipeline	1.5 Hrs.
DevSecOps model for SecOps	• Why the traditional Security Operations Center is no longer effective? • A DevSecOps model for Security Operations • Data analysis, security incident identification and analysis as code • Elastic stack (formerly ELK stack) • Artificial Intelligence, machine learning and data discovery tools • Security Incident Response as code Red Teams and Blue Teams • Real-life Cloud Security Issues • Demo: Operational cloud security issues Lab : OpenSCAP	3 Hrs.
People aspects of DevSecOps	• Culture • Organization • Skills and training • Security champions • Recruitment • Team effectiveness	1 Hr.