DevSecOps Engineering (DSOE)℠

DURATION - 16 Hours

Learn the purpose, benefits, concepts, and vocabulary of DevSecOps including DevOps security strategies and business benefits.

OVERVIEW

As companies are pushing code faster and more often than ever, the rate of vulnerabilities in our systems is accelerating. As we are being asked to do more with less, DevOps has shown immense value to business and security as an integral component that needs to be integrated into the strategy.

Topics covered in the course include how DevSecOps provides the business value of DevOps and the ability DevOps has to enable the business and support an organizational transformation with the ultimate goal of increasing productivity, reducing risk, and optimizing cost in the organization.

This course explains how DevOps security practices differ from other security approaches and provides the education needed to understand and apply data and security sciences. Participants learn the purpose, benefits, concepts, and vocabulary of DevSecOps; particularly how DevSecOps roles fit with a DevOps culture and organization. At the end of this course, participants will understand using "security as code" with the intent of making security and compliance consumable as a service.

The course is designed to teach practical steps on how to integrate security programs into DevOps practices and highlights how professionals can use data and security science as the primary means of protecting the organization and customer.

Using real-life scenarios and case studies, participants will have tangible takeaways to leverage when back at the office.

This course positions learners to successfully complete the DevSecOps Engineering exam, which is offered on the last day of class for classroom learners. Virtual learners will receive a voucher for a webcam proctored exam which they can schedule at their convenience.

COURSE 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

AUDIENCE

The target audience for the DevSecOps Engineering course are professionals including:

- Anyone involved or interested in learning about DevSecOps strategies and automation
- Anyone involved in Continuous Delivery toolchain architectures
- Compliance Team
- Delivery Staff
- DevOps Engineers
- IT Managers
- IT Security Professionals, Practitioners, and Managers
- Maintenance and support staff
- Managed Service Providers
- Project & Product Managers
- Quality Assurance Teams
- Release Managers
- Scrum Masters
- Site Reliability Engineers
- Software Engineers
- Testers

LEARNER MATERIALS

- Sixteen (16) hours of instructor-led training and exercise facilitation
- Digital Learner Manual (excellent post-class reference)
- Participation in exercises designed to apply concepts
- Sample documents, templates, tools and techniques
- Access to additional sources of information and communities

PREREQUISITES

An understanding and knowledge of common DevOps terminology and concepts and related work experience are recommended**.**

CERTIFICATION EXAM

Successfully passing (65%) the 90-minute examination, consisting of 40 multiple-choice questions, leads to the candidate's designation as a certified DevSecOps Engineer (DSOE). The certification is governed and maintained by the DevOps Institute.

COURSE OUTLINE

- Course Introduction
  - Course Goals
  - Course Agenda
  - *Exercise*: Diagramming Your CI/CD Pipeline
- Why DevSecOps?
  - Key Terms and Concepts
  - Why DevSecOps is important
  - 3 Ways to Think About DevOps+Security
  - Key Principles of DevSecOps
- Culture and Management
  - Key Terms and Concepts
  - Incentive Model
  - Resilience
  - Organizational Culture
  - Generativity
  - Erickson, Westrum, and LaLoux
  - *Exercise*: Influencing Culture
- Strategic Considerations
  - Key Terms and Concepts
  - How Much Security is Enough?
  - Threat Modeling
  - Context is Everything
  - Risk Management in a High-velocity World
  - *Exercise*: Measuring For Success
- General Security Considerations
  - Avoiding the Checkbox Trap
  - Basic Security Hygiene
  - Architectural Considerations
  - Federated Identity
  - Log Management
- IAM: Identity & Access Management
  - Key Terms and Concepts
  - IAM Basic Concepts
  - Why IAM is Important
  - Implementation Guidance
  - Automation Opportunities
  - How to Hurt Yourself with IAM
  - *Exercise*: Overcoming IAM Challenges
- Application Security
  - Application Security Testing (AST)
  - Testing Techniques
  - Prioritizing Testing Techniques
  - Issue Management Integration
  - Threat Modeling
  - Leveraging Automation
- Operational Security
  - Key Terms and Concepts
  - Basic Security Hygiene Practices
  - Role of Operations Management
  - The Ops Environment

- *Exercise*: Adding Security to Your CI/CD Pipeline
- Governance, Risk, Compliance (GRC) and Audit
  - Key Terms and Concepts
  - What is GRC?
  - Why Care About GRC?
  - Rethinking Policies
  - Policy as Code
  - Shifting Audit Left
  - 3 Myths of Segregation of Duties vs. DevOps
  - *Exercise*: Making Policies, Audit and Compliance Work with DevOps
- Logging, Monitoring, and Response
  - Key Terms and Concepts
  - Setting Up Log Management
  - Incident Response and Forensics
  - Threat Intelligence and Information Sharing
- Course Review
  - Where We Started
  - What We Covered
  - Key Reminders of What's Important
  - *Exercise*: Creating a Personal Action Plan
- Exam Preparations
  - Exam Requirements, Question Weighting, and Terminology List
  - Sample Exam Review