

DevSecOps Engineering (DSOE)

Length: 2 Days

Summary: 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.

Course Objectives: 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

Who Should Attend: 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

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

COURSE CONTENT

- 1: WHY DEVSECOPS?**
 - Key Terms and Concepts
 - Why DevSecOps is important
 - 3 Ways to Think About DevOps+Security
 - Key Principles of DevSecOps
- 2: CULTURE AND MANAGEMENT**
 - Key Terms and Concepts
 - Incentive Model
 - Resilience
 - Organizational Culture
 - Generativity
 - Erickson, Westrum, and LaLoux
 - Exercise: Influencing Culture
- 3: 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
- 4: GENERAL SECURITY CONSIDERATIONS**
 - Avoiding the Checkbox Trap
 - Basic Security Hygiene
 - Architectural Considerations
 - Federated Identity
 - Log Management
- 5: 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
- 6: APPLICATION SECURITY**
 - Application Security Testing (AST)
 - Testing Techniques
 - Prioritizing Testing Techniques
 - Issue Management Integration
 - Threat Modeling
 - Leveraging Automation
- 7: 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
- 8: 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
- 9: LOGGING, MONITORING, AND RESPONSE**
 - Key Terms and Concepts
 - Setting Up Log Management
 - Incident Response and Forensics
 - Threat Intelligence and Information Sharing