DevSecOps Foundation(SM)

This course is presented in association with DevOps Institute.

Duration: 2 Days

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

Who Should Attend

The DevSecOps course is designed for:

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

Learning Outcomes

The objectives for DevSecOps include an understanding of:

- The purpose, benefits, concepts, and vocabulary
- 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 organisation

Course Contents

1. Course Introduction

- Course Goals
- Course Agenda
- Exercise: Diagramming Your CI/CD Pipeline

2. Why DevSecOps?

- Key Terms and Concepts
- Why DevSecOps is important
- 3 Ways to Think About DevOps+Security
- Key Principles of DevSecOps

3. Culture & Management

- Incentive Model
- Resilience
- Organisational Culture
- Generativity
- Erickson, Westrum, and LaLoux
- Exercise: Influencing Culture

4. Strategic Considerations

- How Much Security is Enough?
- Threat Modeling
- Context is Everything
- Risk Management in a High-velocity World
- Exercise: Measuring For Success

5. General Security Considerations

- Avoiding the Checkbox Trap
- Basic Security Hygiene
- Architectural Considerations
- Federated Identity
- Log Management

6. IAM: Identity & Access Mgmt

- IAM Basic Concepts
- Why IAM is Important
- Implementation Guidance
- Automation Opportunities
- How to Hurt Yourself with IAM
- Exercise: Overcoming IAM Challenges

7. Application Security

- Application Security Testing (AST)
- Testing Techniques
- Prioritising Testing Techniques
- Issue Management Integration
- Threat Modeling
- Leveraging Automation

8. Operational Security

- Basic Security Hygiene Practices
- Role of Operations Management
- The Ops Environment
- Exercise: Adding Security to Your CI/CD Pipeline

9. GRG & Audit

- 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

10. Logging, Monitoring & Response

- Setting Up Log Management
- Incident Response and Forensics
- Threat Intelligence and Information Sharing