DevSecOps Foundation® (DSOF)

Course Content -

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