DevSecOps and Cloud Security
By Dr. Vishwanath Rao

Prerequisites

- Basic understanding of software development and security concepts
- Familiarity with DevOps tools and practices
- Basic understanding of cloud computing and containerization

Target Audience

- Software developers
- DevOps engineers
- Security professionals
- IT professionals
- Anyone interested in learning about DevSecOps and its applications in modern software development

Day 1: Introduction to DevSecOps and Security Fundamentals

- Morning:
  - Introduction to DevSecOps
    - Definition and importance of DevSecOps
    - Overview of the DevSecOps lifecycle: Plan, Build, Test, Deploy, Operate
  - Security Fundamentals
    - Confidentiality, Integrity, Availability, Authentication, Authorization, and Accounting (CIAA)
    - Threat modeling and risk assessment
    - Security principles: Least Privilege, Separation of Duties, and Defense in Depth
- Afternoon:
  - Hands-on Exercise: Creating a Simple CI/CD Pipeline using Jenkins or GitLab CI/CD
    - Introduction to CI/CD pipelines
    - Creating a simple pipeline using Jenkins or GitLab CI/CD
  - Introduction to Security Testing
    - Static Application Security Testing (SAST)
    - Dynamic Application Security Testing (DAST)
    - Interactive Application Security Testing (IAST)

Day 2: Secure Coding and Secure Development

- Morning:
  - Secure Coding Practices
    - Secure coding guidelines
    - Secure coding standards

        - Secure coding tools: CodeSonar, FindBugs, and SonarQube
    - Secure Development Lifecycle
        - Secure requirements
        - Secure design
        - Secure implementation
        - Secure testing
- Afternoon:
    - Hands-on Exercise: Writing Secure Code using Secure Coding Practices and Secure Coding Tools
        - Writing secure code using secure coding practices and tools
        - Reviewing and testing secure code
    - Introduction to Secure Development Methodologies
        - Secure Agile
        - Secure Scrum
        - Secure Waterfall

Day 3: Container Security and Orchestration

- Morning:
    - Container Security
        - Container security threats
        - Container security best practices
        - Container security tools: Docker Security Scanning, Kubernetes Network Policies, and Falco
    - Container Orchestration
        - Kubernetes
        - Docker Swarm
        - Apache Mesos
- Afternoon:
    - Hands-on Exercise: Creating a Containerized Application using Docker and Kubernetes
        - Creating a containerized application using Docker and Kubernetes
        - Reviewing and testing the containerized application
    - Introduction to Container Networking
        - Container networking fundamentals
        - Container networking protocols
        - Container networking tools: Docker Compose and Kubernetes Network Policies

Day 4: Cloud Security and Compliance

- Morning:
    - Cloud Security
        - Cloud security threats
        - Cloud security best practices
        - Cloud security tools: AWS IAM, Azure Active Directory, and Google Cloud Identity and Access Management
    - Cloud Compliance

        - Cloud compliance frameworks: PCI-DSS, HIPAA, and GDPR
        - Cloud compliance regulations: AWS Well-Architected Framework, Azure Compliance Framework, and Google Cloud Compliance Framework
- Afternoon:
    - Hands-on Exercise: Creating a Cloud-Based Application using AWS or Azure
        - Creating a cloud-based application using AWS or Azure
        - Reviewing and testing the cloud-based application
    - Introduction to Cloud Security Architectures
        - Cloud security architectures for AWS, Azure, and Google Cloud
        - Cloud security architecture best practices

Day 5: DevSecOps Tools and Automation

- Morning:
    - DevSecOps Tools
        - Jenkins
        - GitLab CI/CD
        - CircleCI
    - Automation
        - Automation frameworks: Ansible, Puppet, and Chef
        - Automation tools: Jenkins, GitLab CI/CD, and CircleCI
- Afternoon:
    - Hands-on Exercise: Creating a CI/CD Pipeline using Jenkins or GitLab CI/CD
        - Creating a CI/CD pipeline using Jenkins or GitLab CI/CD
        - Reviewing and testing the CI/CD pipeline
    - Introduction to DevSecOps Platforms
        - GitLab DevSecOps
        - CircleCI DevSecOps
        - AWS DevSecOps

Additional Topics

- Secure Testing
    - Secure testing methodologies
    - Secure testing tools: Burp Suite, ZAP, and OWASP ZAP
    - Secure testing best practices
- Secure Monitoring
    - Secure monitoring tools: ELK Stack, Splunk, and Sumo Logic
    - Secure monitoring best practices
    - Secure monitoring architectures
- Secure Incident Response
    - Secure incident response methodologies
    - Secure incident response tools: Splunk, Sumo Logic, and ELK Stack
    - Secure incident response best practices