DevSecOps Foundation

Curriculum 5 Days

Day - 1

Introduction to DevSecOps

- Problem Statement: Understanding the need for integrating security into DevOps.
- Overview: What is DevSecOps and why it matters.
- Tools: Introduction to popular DevSecOps tools and their roles.

DevSecOps Principles and Culture

- Problem Statement: Bridging the gap between development, operations, and security teams.
- Core Principles: Shift-left security, continuous security, automation.
- Tools: Overview of tools supporting cultural change and collaboration (e.g., Slack, Microsoft Teams).

Secure Software Development Lifecycle (SDLC)

- Problem Statement: Incorporating security into each phase of SDLC.
- Phases: Planning, development, testing, deployment, maintenance.
- Tools: Microsoft Azure DevOps, GitHub, GitLab.
- Hands-on: Setting up a secure SDLC pipeline.

Threat Modeling and Risk Management

- Problem Statement: Identifying and mitigating potential security threats early.
- Techniques: STRIDE, DREAD, PASTA.
- Tools: OWASP Threat Dragon, Microsoft Threat Modeling Tool.
- Hands-on: Creating a threat model for a sample application.

Day - 2

Static Application Security Testing (SAST)

- Problem Statement: Detecting security issues in the codebase.
- Introduction: Importance of SAST in DevSecOps.
- Tool: SonarQube.
- Hands-on: Integrating SonarQube with CI/CD pipeline for static code analysis.

Dynamic Application Security Testing (DAST)

- Problem Statement: Identifying vulnerabilities in running applications.
- Introduction: How DAST complements SAST.
- Tool: OWASP ZAP.
- Hands-on: Running dynamic tests with OWASP ZAP

Software Composition Analysis (SCA)

- Problem Statement: Managing vulnerabilities in open-source components.
- Introduction: Importance of SCA in modern applications.
- Tool: Snyk.
- Hands-on: Scanning dependencies with Snyk.

Interactive Application Security Testing (IAST)

- Problem Statement: Combining SAST and DAST for better security coverage.
- Introduction: How IAST works in real-time.
- Tool: Contrast Security.
- Hands-on: Setting up IAST with Contrast Security.

Day - 3

CI/CD Pipeline Security

- Problem Statement: Ensuring security within continuous integration and deployment processes.
- Introduction: Best practices for securing CI/CD pipelines.
- Tools: Jenkins, GitLab CI/CD.
- Hands-on: Securing a CI/CD pipeline with Jenkins and GitLab CI/CD.

Container Security

- Problem Statement: Protecting containerized applications.
- Introduction: Security challenges with Docker and Kubernetes.
- Tool: Aqua Security.
- Hands-on: Implementing container security with Aqua Security.

Infrastructure as Code (IaC) Security

- Problem Statement: Securing infrastructure managed by code.
- Introduction: Best practices for securing IaC.
- Tool: Terraform with Checkov.
- Hands-on: Securing Terraform configurations with Checkov.

Secret Management

- Problem Statement: Managing secrets securely in DevOps pipelines.
- Introduction: Importance of secret management.
- Tool: HashiCorp Vault.
- Hands-on: Implementing secret management with HashiCorp Vault.

Day - 4

Continuous Monitoring

- Problem Statement: Detecting and responding to security incidents in real-time.
- Introduction: Key metrics and logging practices.
- Tools: ELK Stack (Elasticsearch, Logstash, Kibana).
- Hands-on: Setting up continuous monitoring with ELK Stack.

Security Information and Event Management (SIEM)

- Problem Statement: Centralizing and analyzing security data.
- Introduction: Benefits of SIEM in DevSecOps.
- Tool: Splunk.
- Hands-on: Configuring SIEM with Splunk.

Incident Response Automation

- Problem Statement: Automating incident response to reduce reaction time.
- Introduction: Key steps in incident response.
- Tool: Palo Alto Networks XSOAR.
- Hands-on: Automating incident response with XSOAR.

Compliance and Auditing

- Problem Statement: Ensuring compliance with industry standards.
- Introduction: Key compliance frameworks (e.g., GDPR, HIPAA).
- Tool: Chef InSpec.
- Hands-on: Using Chef InSpec for compliance checks.

Day - 5

Advanced Threat Detection

- Problem Statement: Identifying sophisticated security threats.
- Introduction: Advanced threat detection techniques.
- Tool: CrowdStrike.
- Hands-on: Using CrowdStrike for advanced threat detection.

Automated Security Orchestration

- Problem Statement: Coordinating multiple security tools and processes.
- Introduction: Benefits of security orchestration.
- Tool: Demisto.
- Hands-on: Implementing security orchestration with Demisto.

Metrics and Reporting

- Problem Statement: Measuring and reporting on security performance.
- Introduction: Key metrics for DevSecOps.
- Tool: Grafana.
- Hands-on: Creating security dashboards with Grafana.

Mock Exam and Certification Preparation

- Review: Recap of key concepts and tools.
- Mock Exam: Practice certification exam.
- Review Session: Going over answers and explanations.
- Final Q&A: Addressing any remaining questions.