DevSecOps Training Program (Windows Platform-Focused)

Duration: 5 Days (8 Hours/Day)
Total Hours: 40 Hours
Audience: Developers, DevOps Engineers, Security Engineers working with Windows-based applications (.NET, WebUI, or other Windows-supported tech stacks)

Day 1: Introduction to DevSecOps & Secure Development on Windows

1.1 Understanding DevSecOps

- What is DevSecOps?
- Shift-left security and why it matters
- DevSecOps lifecycle
- Key differences for Windows-based ecosystems

1.2 Windows Environment for Secure DevOps

- Windows architecture essentials
- Deployment options: .NET, IIS, Windows-native containers, desktop apps, WebUI-based apps
- PowerShell and Windows Terminal for automation
- Secure coding principles for Windows-supported technologies

1.3 Secure SDLC on Windows

- Integrating security in the SDLC
- Threat modeling (STRIDE, DREAD)
- Microsoft SDL

Hands-on:

- Setting up a secure Dev environment (Visual Studio, PowerShell, Windows Server)
- Threat modeling with Microsoft Threat Modeling Tool

Day 2: Jenkins-Powered CI/CD & DevSecOps on Windows (Full Day)

2.1 Jenkins for Windows CI/CD

- Installing and configuring Jenkins on Windows
- Running Jenkins agents on Windows

- Building pipelines for .NET, WebUI, and PowerShell-based apps

2.2 Secure Jenkins Configuration

- RBAC and role segregation
- Plugin security and update strategy
- Jenkinsfile best practices for Windows

2.3 Security Gates in Jenkins

- Integrating SAST, SCA, and custom security tools in pipelines
- Jenkins audit trails, logs, and hardening tips

Hands-on:

- Complete Windows Jenkins pipeline setup
- Secure Jenkins agent configuration and credential management

---

Day 3: Static & Dynamic Security Testing (SAST & DAST)

3.1 Static Application Security Testing (SAST)

- Introduction to SAST
- Open-source tools: SonarQube, CodeQL, Bandit (for Python-based Win apps), Gosec (for Go)
- Integrating SonarQube with Jenkins pipelines

3.2 Dynamic Application Security Testing (DAST)

- Introduction to DAST
- Using OWASP ZAP for dynamic scanning
- Automating DAST scans in CI/CD workflows

3.3 Trivy and Other Scanners

- Overview of Trivy for container and file system scanning on Windows
- Software Composition Analysis (SCA) with Trivy, Snyk CLI (if compatible), Dependency-Check

Hands-on:

- Jenkins + SonarQube SAST
- Automating ZAP DAST with Jenkins and local Windows deployments
- Trivy scan of Windows containers or directories

Day 4: Custom Security Tooling & Windows-Specific Hardening

4.1 Custom Security Tool Development

- PowerShell for security automation
- Writing custom vulnerability checkers
- Parsing Windows event logs and registry values for threats

4.2 Infrastructure & OS Security on Windows

- Hardening Windows Servers
- Microsoft Security Compliance Toolkit
- Sysmon, Event Viewer, audit policy

4.3 Application & Network Security

- OWASP Top 10 implementation checks
- Web.config best practices
- Windows Defender Firewall and Network Policies

Hands-on:

- PowerShell-based security tools
- Windows hardening lab (local GPO + security toolkit)
- Auditing logs and events for breach simulation

Day 5: End-to-End DevSecOps Workflow & Compliance

5.1 Building a Secure DevSecOps Pipeline

- Combining Jenkins, SonarQube, Trivy, ZAP
- IAM and secrets management on Windows
- Deployment pipelines with security guardrails

5.2 Compliance and Governance

- Windows Event Logs for compliance audits
- Implementing CIS/NIST on Windows platform
- Documenting and auditing CI/CD security

5.3 Capstone Project

- Group activity: Secure CI/CD pipeline (SAST + DAST + SCA)

    - Jenkins orchestration
    - SonarQube scan
    - ZAP-based DAST
    - Trivy/Dependency-Check for SCA
    - Custom scripts for log parsing, secrets checks

Hands-on:

- Complete CI/CD pipeline with security enforcement
- Report generation and compliance check demo

Outcome: By the end of the 5 days, participants will be able to:

- Implement and enforce DevSecOps practices on Windows
- Use SAST, DAST, SCA, and custom tools in CI/CD
- Harden infrastructure, applications, and networks
- Ensure compliance and security from development to deployment