DevSecOps Training

Module 1: Introduction to DevSecOps

- **1.1 DevOps vs DevSecOps**
- **1.2 Principles of Shift Left Security**
- **1.3 CI/CD Basics and DevSecOps Integration Points**
- *Practical*: Git workflow + CI/CD demo with GitHub Actions.

Module 2: Threat Modeling and Secure Design

- **2.1 OWASP Top 10 Overview**
- **2.2 STRIDE, DREAD, and PASTA Models**
- **2.3 Secure Design Patterns**
- *Tools*: OWASP Threat Dragon (open-source)
- *Activity*: Model a simple web app using Threat Dragon.

Module 3: Secure Coding and SAST

- **3.1 Secure Coding Practices**
- **3.2 Static Application Security Testing**
- *Open-source*: SonarQube, Semgrep
- *Paid Exposure*: Checkmarx, Snyk Code
- *Lab*: Scan a vulnerable Python/Java project with SonarQube and Semgrep.

Module 4: Dependency Management and SCA

- **4.1 Software Composition Analysis**
- **4.2 License and Vulnerability Management**
- *Open-source*: OWASP Dependency-Check, Syft

- *Paid Exposure*: Snyk, Black Duck
- *Lab*: Run SCA scans on a Node.js or Python project.

Module 5: Container and Infrastructure Security

- **5.1 Docker and Kubernetes Security Fundamentals**
- **5.2 Image Scanning & Hardening**
- **5.3 IaC Security**
- *Tools*: Trivy, Dockle, KICS, Checkov
- *Paid Exposure*: Prisma Cloud, Aqua
- *Lab*: Scan Docker images and Terraform code.

Module 6: DAST and API Security

- **6.1 Dynamic Application Security Testing**
- **6.2 API Security Testing**
- *Open-source*: OWASP ZAP, Nikto, Postman
- *Paid*: Burp Suite Pro
- *Lab*: Run OWASP Juice Shop or DVWA in a container and test it.

Module 7: CI/CD Pipeline Security

- **7.1 Secure GitOps & CI/CD Pipelines**
- **7.2 Secrets Management in Pipelines**
- *Tools*: Jenkins + OWASP Dependency-Check, Gitleaks, SOPS, Sealed Secrets
- *Lab*: Build a secure pipeline with GitHub Actions and integrate Gitleaks and Trivy.

Module 8: Monitoring and Runtime Protection

- **8.1 Logging and Audit Trails**

- **8.2 Intrusion Detection in Kubernetes**
- **8.3 Runtime Threat Detection**
- *Tools*: Falco, Prometheus, Loki, Grafana
- *Lab*: Set up Falco on Kubernetes and monitor suspicious behavior.

Module 9: Governance, Risk, and Compliance

- **9.1 DevSecOps in Compliance (PCI-DSS, SOC2, etc.)**
- **9.2 Policy as Code**
- *Tools*: Open Policy Agent (OPA), Conftest
- *Lab*: Enforce Kubernetes admission policies with OPA Gatekeeper.

Module 10: Capstone Project + Assessment

- **10.1 Design & Implement DevSecOps Pipeline**
- **10.2 Secure a Sample Application End-to-End**
- *Task*: Use open-source tools to integrate security into a CI/CD workflow for a real-world project.
- *Optional*: Bonus task to compare results using a paid tool demo.