DevSecOps Professional Syllabus

1- Introduction to DevOps and DevSecOps

- What is DevOps?
- DevOps Building Blocks- People, Process and Technology.
- DevOps Principles - Culture, Automation, Measurement and Sharing (CAMS)
- Benefits of DevOps - Speed, Reliability, Availability, Scalability, Automation, Cost and Visibility.
- What is Continuous Integration and Continuous Deployment?

2- Introduction to the Tools of the trade

- Github/Gitlab/BitBucket
- Docker
- Docker Registry
- Ansible
- Jenkins/Travis/Gitlab CI/Bitbucket
- Gauntlt
- Inspec
- Bandit/retireJS/Nmap

3- Secure SDLC and CI/CD pipeline

- What is Secure SDLC
- Secure SDLC Activities and Security Gates
- DevSecOps Maturity Model (DSOMM)
- Using tools of the trade to do the above activities in CI/CD
- Embedding Security as part of CI/CD pipeline
- DevSecOps and challenges with Pentesting and Vulnerability Assessment.

4- Software Component Analysis (SCA)

- What is Software Component Analysis?
- Software Component Analysis and its challenges.
- What to look in an SCA solution (Free or Commercial).
- Embedding SCA tools like OWASP Dependency Checker, Safety, RetireJs, and NPM Audit, Snyk into the pipeline.
- Demo: using OWASP Dependency Checker to scan third party component vulnerabilities in Java Code Base.

5- Static Analysis(SAST) in CI/CD pipeline.

- What is Static Application Security Testing?
- Static Analysis and its challenges.
- Embedding SAST tools into the pipeline.
- Secrets scanning to prevent secret exposure in the code.
- Writing custom checks to catch secrets leakage in an organization.

6- Dynamic Analysis(DAST) in CI/CD pipeline.

- What is Dynamic Application Security Testing?
- Dynamic Analysis and Its challenges (Session Management, AJAX Crawling)
- Embedding DAST tools like ZAP and Burp Suite into the pipeline.
- SSL misconfiguration testing
- Server Misconfiguration Testing like secret folders and files
- Sqlmap testing for SQL Injection vulnerabilities.

7- Infrastructure as Code and its security.

- What is Infrastructure as Code and its benefits?
- Platform + Infrastructure Definition + Configuration Management.
- Introduction to Ansible.
- Tools and Services which helps to achieve IaaC

8- Compliance as code

- Different approaches to handle compliance requirements at DevOps scale
- Using configuration management to achieve compliance.
- Manage compliance using Inspec/OpenScap at Scale.
- Create an Inspec profile to create compliance checks for your organization
- Use Inspec profile to scale compliance.

9- Vulnerability Management with custom tools

- Approaches to manage the vulnerabilities in the organization.
- Using Defect Dojo for vulnerability management.