

DevSecOps

1 day class

Modern enterprises are implementing the technical and cultural changes required to embrace DevOps methodology. DevSecOps extends DevOps by introducing security early into the SDLC process, thereby minimizing the security vulnerabilities and enhancing the software security posture. In this workshop we will show how this can be achieved through a series of live demonstrations and practical examples.

As part of this workshop attendees will receive a state-of-the-art DevSecOps tool-chest comprising of various open-source tools and scripts to help the DevOps engineers in automating security within the CI/CD pipeline. While the workshop uses Java/J2EE framework, the workshop is language agnostic and similar tools can be used against other application development frameworks.

Why DevSecOps?

The DevSecOps process will help to:

- Create a security culture/mindset amongst the already integrated “DevOps” team.
- Find and fix security bugs as early in SDLC as possible.
- The culture promotes the philosophy “security is everyone’s problem”.
- Integrate all security software centrally and utilize the results more effectively.
- Measure and shrink the attack surface



PREREQUISITES

Our workshop will be delivered as an interactive session, so the attendees only need to carry a laptop with them. We also encourage the attendees to download and try the tools and techniques discussed during the workshop as the instructor is demonstrating it.

CLASS CONTENT

The following topics will be covered encompassing the entire Secure DevOps pipeline

- Introduction and overview of DevOps
- What and Why of DevSecOps?
- Integrating Security in CI/CD
- Vulnerability Management using Archerysec
- Secret Management using Vault, Jenkins and Docker Secrets
- Security in Developer Workstations: Pre-Commit Hooks using Talisman
- Software Composition Analysis using Dependency-Checker
- SAST - Static Application Security Testing using FindSecBugs
- DAST - Dynamic Application Security Testing using ZAP and OpenVAS
- Compliance as Code using Inspec
- Security in Infrastructure as a Code using Clair
- Production Real-Time Alerting and Monitoring using Modsecurity WAF
- DevSecOps in AWS
- Challenges in DevSecOps
- DevSecOps Enablers

WHO SHOULD TAKE THIS CLASS

DevSecOps Workshop, which will give the target audience a holistic approach in assessing and securing the web applications in an automated fashion within the existing CI/CD pipeline, can be attended by DevOps engineers, security and solutions architects, system administrators and anybody who is willing to inject security aspects in their DevOps process.

WHAT STUDENTS SHOULD BRING

A Laptop with Wifi connectivity and admin privileges.

CLASS TAKEAWAY

The attendees will also receive a free DevSecOps tool-chest (designed by the NotSoSecure team) which can be directly implemented in most CI/CD pipeline