

## Day - 1

- **Understanding DevSecOps**

- What is Security?
- Why Security?
- What is DevSecOps?
- Understanding a types of Threat in DevOps
- Why DevSecOps?
- DevOps Security Best Practice Approach
- Understanding a Phases in DevOps and Their Security Concern
- Recommendations for Security Practices in DevSecOps
- Recommendations for Security Tools in DevSecOps

- **DevOps Security Phases?**

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Runtime Application Security Testing (RAST)
- Database Security Scanning
- Mobile Application Security Testing (MAST)

- **DevSecOps Practices**

- DevSecOps Practices with AWS
- DevSecOps Practices with Docker
- DevSecOps Practices with Kubernetes

- **Implementing some of the DevSecOps Tools**

- OWASP SonarQube for Code Scanning [Demo]
- Chef InSpec for Scanning your applications and infrastructure [Demo]
- ELK with Kibana for Log analysis for Security Threat [Demo]
- HashiCorp Vault for security tool for certificates, API keys, or passwords
- Fortify Webinspect for Dynamic Application Security Testing (DAST)
- Fortify Application Defender for Runtime Application Security Testing (RAST)