DELEGATES WILL RECEIVE
The attendees will receive a DevSecOps-Lab VM (designed by the NotSoSecure team) containing all the code, scripts and tools that are used for building the entire DevSecOps pipeline.

COURSE CONTENTS
Introduction to DevOps
• Introduction and Lab Setup
• Challenges with Traditional IT
• What is DevOps?

Introduction to DevSecOps
• Challenges for Security in DevOps
• DevSecOps – Why, What and How?
• Vulnerability Management

Continuous Integration
• Pre-Commit Hooks
• Secrets Management

Continuous Delivery
• Software Composition Analysis (SCA)
• Static Analysis Security Testing (SAST)
• Dynamic Analysis Security Testing (DAST)

Infrastructure As Code
• Vulnerability Assessment (VA)
• Container Security (CS)
• Compliance as Code (CaC)

Continuous Monitoring
• Alerting and Monitoring
• Introduction to F-ELK

DevSecOps in AWS
• DevOps on Cloud Native AWS
• AWS Threat Landscape
• DevSecOps in Cloud Native AWS

DevSecOps Challenges and Enablers
• Challenges with DevSecOps
• Building DevSecOps Culture
• Security Champions

KEY TAKEAWAYS
• Understand how to tackle security issues in a fast-moving DevOps environment
• Identify tools/solutions and develop processes to create a secure by default infrastructure
• Utilize the integration scripts and tools provided in the DevSecOps Lab to create your own DevSecOps pipeline

COURSE OBJECTIVES
• Create a security culture/mindset amongst the already integrated “DevOps” team.
• Find and fix security bugs as early in SDLC as possible
• Build a secure by default infrastructure
• Build a system with continuous security monitoring