DevSecOps 1 Day
Automating Security in DevOps

One Day hands-on training to automate security into a fast-paced DevOps environment using various open-source tools and scripts.

Modern enterprises are implementing the technical and cultural changes required to embrace DevOps methodology by introducing practices such Continuous Integration (CI), Continuous Delivery (CD), Continuous Monitoring (CM) and Infrastructure as Code(IaC) .DevSecOps extends DevOps by introducing security in each of these practices giving a certain level of security assurance in the final product. In this training, we will demonstrate using our state-of-the-art DevSecOps Lab as to how to inject security in CI, CD, CM and IaC.

This is a complete hands-on training with attendees requiring only a browser to complete the entire training. Attendees will receive the DevSecOps Lab built using Vagrant and Ansible comprising of various open-source tools and scripts to help the DevOps engineers in automating security within their CI/CD pipeline.

A Short preview of our course is available for viewing here https://www.youtube.com/watch?v=_iGCZ4NPDqY

Who Should Attend

DevOps engineers, security and solutions architects, system administrators will also strongly benefit from this course as it'll give them a holistic approach towards application security.

Delegate Requirements

Anybody with a background in IT or related to software development whether a developer or a manager can attend this course to get an insight about DevOps and DevSecOps.

Delegates Should Bring

Any device having a browser.

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

NotSoSecure part of
claranet cyber security

For more information:

UK: +44 (0)1223 653 193
Email: contact@notsosecure.com
US: +1 (628) 200-3053/3052
Visit: notsosecure.com

DevSecOps 1 Day (Continued)

Automating Security in DevOps

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

Additional Information

We delivered this training for Virtual OWASP AppSec Days Conference on 28-29th April 2020 with 30 attendees

The training received an overwhelming response at the OWASP AppSec DC event in September 2019 with around 63 registrations.
https://globalappsecdc2019.sched.com/event/SKIC

As well as at the below conferences
https://agiledevopseast.techwell.com/program/tutorials/devsecops-automating-security-devops-agile-devops-east-2019

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**