DevSecOps - Automating Security in DevOps

2 days class

Two Days 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.

Every delegate will be provided a personalized cloud setup of our DevSecOps lab for hands-on implementation of various security tools in the CI/CD/CM pipeline. Attendees will receive the DevSecOps Lab built using Vagrant and Ansible comprising the same tools and scripts as a takeaway.

A Short preview of our course is available for viewing here:

https://www.youtube.com/watch?v=_iGCZ4NPDqY

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 by automating security
- Build a system with continuous security monitoring

COURSE CONTENTS

LAB SETUP
- Online Lab Setup
- Offline Lab Instructions

INTRODUCTION TO DEVOPS
- What is DevOps?
  - o Lab: DevOps Pipeline

INTRODUCTION TO DEVSECOPS
- Challenges for Security in DevOps
- DevOps Threat Model
- DevSecOps – Why, What and How?
- Vulnerability Management

CONTINUOUS INTEGRATION
- Pre-Commit Hooks
  - o Introduction to Talisman
  - o Lab: Running Talisman
  - o Lab: Create your own regexes for Talisman
- Secrets Management
  - o Introduction to HashiCorp Vault
  - o Demo: Vault Commands

CONTINUOUS DELIVERY
- Software Composition Analysis (SCA)
  - o Introduction to Dependency-Check
  - o Lab: Run Dependency-Check pipeline
  - o Lab: Fix issues reported by Dependency-Check
- Static Analysis Security Testing (SAST)
  - o Introduction to Semgrep
  - o Lab: Run Semgrep pipeline
  - o Lab: Create your own Semgrep Rules
  - o Lab: Fix Issues reported by Semgrep
- Dynamic Analysis Security Testing (DAST)

- Introduction to OWASP ZAP
- Demo: Creating ZAP Context File
- Lab: Run ZAP in pipeline Infrastructure As Code

• Vulnerability Assessment (VA)
- Introduction to OpenVAS
- Lab: Run OpenVAS pipeline

• Container Security (CS)
- Introduction to Trivy
- Lab: Run Trivy in Pipeline
- Lab: Improvise Docker base image

• Compliance as Code (CaC)
- Introduction to Inspec
- Lab: Run Inspec in Pipeline
- Lab: Improvise Docker compliancy controls

CONTINUOUS MONITORING

• Logging
- Introduction to the ELK Stack
- Lab: View Logs in Kibana

• Alerting
- Introduction to ElastAlert and ModSecurity
- Lab: View Alerts in Kibana

• Monitoring
- Lab: Create Attack Dashboards in Kibana

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
• Case Studies
• Where do we Begin?
• DevSecOps Maturity Model

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
- In-depth understanding of various tools that can be used for security automation
- Utilize the integration scripts and tools provided in the DevSecOps Lab to create your own DevSecOps pipeline

WHO SHOULD TAKE THIS COURSE?

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. Audience Skill Level Intermediate Student 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.

WHAT STUDENTS SHOULD BRING

- Any laptop with a browser
- In order to access our labs you'll need an unfiltered direct connection to the internet. Our labs will not be accessible from behind a proxy or a firewalled internet connection

WHAT STUDENTS WILL BE PROVIDED WITH

Access to cloud DevSecOps-Lab for 24 hours post end of the training for further hands-on practice to each delegate The attendees will also 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.

NotSoSecure part of claranet cyber security