Implementing DevSecOps

- Learn how to build security into your DevOps process
- Learn how to use security requirements to plan your testing efforts
- Explore key aspects of security testing – web security, threat modeling, risk assessment
- Learn how security testing can be effectively leveraged within a DevOps pipeline
- Understand how DevSecOps builds upon DevOps practices
- Understand how technical and automation skills can be leveraged in your DevSecOps efforts
- Develop practical experience through the completion of hands-on exercises

Your organization has started moving toward a DevOps way of thinking and working, and you have started to set up a delivery pipeline. However, you realize that security testing is missing from your pipeline, and you know that testing for security early and often is an important part of ensuring that your system is free from vulnerabilities.

If you are looking for a way to include security testing in your pipeline and turn your DevOps practice into a DevSecOps practice, then this course is for you. You will learn how DevSecOps builds upon the principles and practices of DevOps and how to integrate security testing tools into the various stages of the pipeline. This course will give you hands-on practice with configuring and using these tools so that you will be prepared to introduce DevSecOps to your own organization.

Who Should Attend?
This course is appropriate for software professionals who are involved with development, testing, security, and operations and who want to incorporate security testing into their organization's pipeline. Because this course has a heavy focus on hands-on exercises, it is most appropriate for practitioners and will not be tailored toward management or leadership.

Laptop Required
This class involves hands-on activities using sample software to better facilitate learning. Each student should bring a laptop with an SSH or PuTTY client preinstalled. Connection specifics and credentials will be supplied during class. Please verify permissions with your IT Admin before class. If you or your Admin have questions about the specific applications involved, contact our Client Support team [1].

Course Outline

DevOps Refresher
Description
Purpose
Goals
Dev vs. Ops
DevOps Principles

Security Refresher
Definition of Information Security
History of Information Security
CIA++
State of Application Security

DevSecOps Overview

Log Management
Description
Motivation
Tools
Log Management Exercise

Monitoring
Description
Motivation
Tools
Monitoring Exercise

Security Information and Event Management (SIEM)
Description

Definition
Relevant Terms
Purpose
Benefits and Drawbacks
Tool Types

Risk Assessment
Importance of Software Security
Understanding Risk
Risk Assessment Exercise

Threat Modeling
Microsoft STRIDE
Architectural and Design Reviews
Threat Modeling Exercise

Software Composition Analysis (SCA)
Description
Motivation
Tools
SCA Exercise

Static Application Security Testing (SAST)
What It Is
Why We Need It
Goals
Pros and Cons
Tools
SAST Exercise

Dynamic Application Security Testing (DAST)
What It Is
Goals
How DAST Tools Work
Pros and Cons
Tools
DAST Exercise

Motivation
Tools
SIEM Exercise

Security Requirements Testing
Functional vs. Non-functional Requirements
Misuse and Abuse Cases
Testing Security Requirements
Security Requirements Exercise

Advanced Techniques: IAST, RASP, and HAST
What They Are
Goals
How These Tools Work
Pros and Cons
Tools

Penetration Testing
What It Is
When It Should be Performed
How It Works
Enumeration and Footprint Analysis
Tool Categories
Pen Testing Exercise

Price: $1545