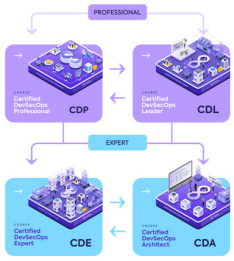


# LUMIFY WORK Self Paced Practical DevSecOps Professional User Guide



IT SERVICE MANAGEMENT AND DEVOPS

Contents



## Practical DevSecOps Professional Self-paced

| INCLUSIONS | LENGTH | PRICE (Incl. GST) |
|---|---|---|
| Exam voucher | 60-day lab access | $1,430 |

**PRACTICAL DEVSECOPS AT LUMIFY WORK**

Practical DevSecOps are the DevSecOps pioneers. Learn DevSecOps concepts, tools, and techniques from industry experts, and master real-world skills in state-of-the-art online labs. Demonstrate your expertise to organisations by earning DevSecOps Certification, with task-based knowledge rather than theory.

Lumify Work is an Official Training Partner of Practical DevSecOps.

## WHY STUDY THIS COURSE

We have all heard about DevSecOps, Shifting Left, Rugged DevOps but there are no clear examples or frameworks available for security professionals to implement in their organisation.
This hands-on course will teach you exactly that – tools and techniques to embed security as part of the DevOps pipeline. We will learn how unicorns like Google, Facebook, Amazon, and Etsy handle security at scale and what we can learn from them to mature our security programs.
In DevSecOps Professional training you will learn how to handle security at scale using DevSecOps practices. We will start off with the basics of DevOps and DevSecOps, then move towards advanced concepts such as Security as Code, Compliance as Code, Configuration Management, Infrastructure as Code, and more.

This self-paced course will provide you with:
**Lif et ime Access:**

- Course manual
- Course videos and checklists
- A 30-minute session with instructors
- Access to a dedicated slack channel
- 30+ guided exercises

**Lab and Exam:**

- 60 days of browser-based lab access
- One exam attempt for Certified DevSecOps Professional (CDP) Certification


My instructor was great being able to put scenarios into real world instances that related to my specific situation.
I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.
I learnt a lot and felt it was important that my goals by attending this course were met.
Great job Lumify Work team.

**AMANDA NICOL**
IT SUPPORT SERVICES MANAGER – HEALT H WORLD LIMIT ED

## WHAT YOU'LL LEARN

- Create a culture of sharing and collaboration among the stakeholders
- Scale security team's effort to reduce the attack surface
- Embed security as part of DevOps and CI/CD

- Start or mature your application security program using modern Secure SDLC practices
- Harden infrastructure using Infrastructure as Code and maintain compliance using Compliance as Code tools and techniques
- Consolidate and co-relate vulnerabilities to scale false-positive analysis using automated tools

**Lumify Work Customised Training**
We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.
For more information, please contact us on 1 800 853 276.

## COURSE SUBJECTS

### Int roduct ion t o DevOps and DevSecOps

- What is DevOps?
- DevOps Building Blocks – People, Process and Technology
- DevOps Principles – Culture, Automation, Measurement and Sharing (CAMS)
- Benefits of DevOps – Speed, Reliability, Availability, Scalability, Automation, Cost and Visibility
- What is Continuous Integration and Continuous Deployment ?
- Continuous Integration to Continuous Deployment to Continuous Delivery
- Continuous Delivery vs Continuous Deployment
- General workflow of CI/CD pipeline
- Blue/Green deployment strategy
- Achieving full automation
- Designing a CI/CD pipeline for a web application
- Common Challenges faced when using DevOps principle
- Case studies on DevOps of cutting edge technology at Facebook, Amazon, and Google
- Demo : A full enterprise-grade DevSecOps Pipeline

### Int roduct ion to the Tools of the Trade

- Github/Gitlab/Bitbucket
- Docker
- Docker Registry
- Ansible
- Jenkins/Travis/Gitlab CI/Bitbucket
- Gauntlt
- Inspec
- Bandit /retireJS/Nmap
- Hands-on Lab: Use Vagrant to practice Infrastructure as a Code
- Hands-on Lab: Building a CI Pipeline using Jenkins/Travis and GitHub/Bitbucket
- Hands-on Lab: Use the above tools to create a complete CI/CD pipeline

### Secure SDLC and CI/CD Pipeline

- What is Secure SDLC?
- Secure SDLC Activities and Security Gates
- Security Requirements (Requirements)
- T hreat Modelling (Design)
- Static Analysis and Secure by Default (Implementation)
- Dynamic Analysis (Testing)
- OS Hardening, Web/Application Hardening (Deploy)
- Security Monitoring/Compliance (Maintain)
- DevSecOps Maturity Model (DSOMM)
- Maturity levels and tasks involved
- 4 -axes in DSOMM
- How to go from Maturity Level 1 to Maturity Level 4
- Best practices for Maturity Level 1
- Considerations for Maturity Level 2
- Challenges in Maturity Level 3
- Dream of achieving Maturity Level 2
- Using tools of the trade to do the above activities in CI/CD
- Embedding Security as part of CI/CD pipeline
- DevSecOps and challenges with Pentesting and Vulnerability Assessment
- Hands-on Lab: Create a CI/CD pipeline suitable for modern applications
- Hands-on Lab: Manage the findings in a fully automated pipeline

**Sof t ware Component Analysis (SCA) in CI/CD Pipeline**

- What is Software Component Analysis?
- Software Component Analysis and its challenges
- What to look for in an SCA solution (free or commercial)
- Embedding SCA tools like OWASP Dependency Checker, Safety, RetireJs, and NPM Audit, Snyk into the pipeline
- Demo : using OWASP Dependency Checker to scan third party component vulnerabilities in Java® Code Base
- Hands-on Lab: using RetireJS and NPM to scan third party component vulnerabilities in JavaScript Code Base
- Hands-on Lab: using Safety/pip to scan third party component vulnerabilities in Python Code Base

**SAST (St at ic Analysis) in CI/CD Pipeline**

- What is Static Application Security Testing?
- Static Analysis and its challenges
- Embedding SAST tools into the pipeline
- Secrets scanning to prevent secret exposure in the code
- Writing custom checks to catch secrets leakage in an organisation
- Hands-on Lab: using SpotBugs to scan Java code
- Hands-on Lab: using Trufflehog/Gitrob to scan for secrets in CI/CD pipeline
- Hands-on Lab: using brakeman/bandit to scan Ruby on Rails and Python Code Base

**DAST (Dynamic Analysis) in CI/CD Pipeline**

- What is Dynamic Application Security Testing?
- Dynamic Analysis and its challenges (Session Management, AJAX Crawling)
- Embedding DAST tools like ZAP and Burp Suite into the pipeline
- SSL misconfiguration testing
- Server Misconfiguration Testing like secret folders and files
- Sqlmap testing for SQL Injection vulnerabilities
- Hands-on Lab: using ZAP to configure per commit /weekly/monthly scans
- Demo : using Burp Suite to configure per commit /weekly/monthly scans

**Inf rast ruct ure as Code and It s Security**

- What is Infrastructure as Code and its benefits?
- Platform + Infrastructure Definition + Configuration Management
- Introduction to Ansible
- Benefits of Ansible
- Push and Pull based configuration management systems
- Modules, tasks, roles, and Playbooks
- Tools and Services which helps to achieve IaaC
- Hands-on Lab: Vagrant, Docker, and Ansible
- Hands-on Lab: Using Ansible to create Golden images and harden infrastructure

**Compliance as Code**

- Different approaches to handle compliance requirements at DevOps scale
- Using configuration management to achieve compliance
- Manage compliance using Inspec/OpenScap at Scale
- Hands-on Lab: Create an Inspec profile to create compliance checks for your organisation
- Hands-on Lab: Use Inspec profile to scale compliance

**Vulnerability Management wit h Cust om Tools**

- Approaches to manage the vulnerabilities in the organisation
- Hands-on Lab: Using Defect Dojo for vulnerability management

## WHO IS THE COURSE FOR?

T his course is aimed at anyone who is looking to embed security as part of agile/cloud/DevOps environments, such as Security Professionals, Penetration Testers, IT Managers, Developers and DevOps Engineers.

## PREREQUISITES

There are no required prerequisites to undertake this course, however students will benefit from having basic knowledge of Linux commands such as ls, cd, mkdir, etc, and application security practices such as OWASP Top

10.

The s upply of this cours e by Lumify Work is governed by the booking terms and conditions . Pleas e read the terms and conditions carefully before enrolling in this cours e, as enrolment in the cours e is conditional on acceptance of thes e terms and conditions .

https://www.lumifywork.com/en-au/courses/practical-devsecops-professional/

Call 1800 853 276 and speak to a Lumify Work Consultant today!

training@lumifywork.com

lumifywork.com

facebook.com/LumifyWorkAU

linkedin.com/company/lumify-work

twitter.com/LumifyWorkAU

youtube.com/@lumifywork

## Documents / Resources

| | |
|---|---|
|  | LUMIFY WORK Self Paced Practical DevSecOps Professional [pdf] User Guide<br>Self Paced Practical DevSecOps Professional, Paced Practical DevSecOps Professional, Prac tical DevSecOps Professional, DevSecOps Professional, Professional |

## References

- Lumify Work | Lumify Work AU
- Lumify Work | Lumify Work AU
- Practical DevSecOps Professional - Self-paced | Lumify Work AU
- User Manual