Manuals+ — User Manuals Simplified.

LUMIFY WORK Self Paced Practical DevSecOps Expert User Guide

Contents

LUMIFY WORK Self-Paced Practical DevSecOps Expert

Product Information

- **Product Name:** Practical DevSecOps Expert Self-paced
- **Inclusions:** Exam voucher
- **Length:** 60-day lab access
- **Price (Incl. GST):** $2 051.50

About Practical DevSecOps

Practical DevSecOps is a pioneering course that teaches DevSecOps concepts, tools, and techniques from industry experts. It offers real-world skills training through state-of-the-art online labs. By earning a DevSecOps Certification, you can demonstrate your expertise to organizations. Lumify Work is an Official Training Partner of Practical DevSecOps.

Why Study This Course?

This advanced DevSecOps Expert training is designed to help security professionals handle security at scale using DevSecOps practices. The course covers the basics of DevOps and DevSecOps, as well as advanced concepts such as Threat Modelling as Code, RASP/IAST, Container Security, Secrets Management, and more.

This self-paced course provides the following:

- Lifetime Access to 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 Expert (CDE) Certification

What You'll Learn

- Create a culture of sharing and collaboration among 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

Product Usage Instructions

To make the best use of the Practical DevSecOps Expert Self-paced course, follow these instructions:

Step 1: Accessing Course Materials

1. Ensure you have a stable internet connection.
2. Visit the course website at **https://www.lumifywork.com/en-au/courses/practical-devsecops-expert/**.
3. Login to your account using the provided credentials.
4. Access the course manual, videos, and checklists for lifetime

Step 2: Interacting with Instructors

As part of the course, you have the opportunity to schedule a 30-minute session with instructors. Follow these steps:

1. Join the dedicated Slack channel provided.
2. Coordinate with the instructors to schedule your session.
3. During the session, ask questions, seek clarification, and

Step 3: Completing Guided Exercises

The course includes 30+ guided exercises to reinforce your learning. Follow these steps:

1. Access the browser-based lab environment using the provided credentials.
2. Follow the instructions provided for each exercise.
3. Practice the concepts, tools, and techniques in a real-world simulated environment.

Step 4: Taking the Exam

After completing the guided exercises and feeling confident in your knowledge, you can attempt the Certified

DevSecOps Expert (CDE) Certification exam. Here's what you need to know:

1. The exam is conducted online.
2. You have 60 days of lab access to prepare for the exam.
3. Login to the exam portal using the provided credentials.
4. Follow the instructions to complete the exam within the allotted time.
5. Upon passing the exam, you will be awarded the Certified DevSecOps Expert (CDE) Certification.

PRACTICAL DEVELOPMENT 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, and Rugged DevOps but there are no clear examples or frameworks available for security professionals to implement in their organization.
T his 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 our advanced DevSecOps Expert 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 threat Modelling as Code, RASP/IAST, Container Security, Secrets Management, and more. This self-paced course will provide you with:

Lifetime Access

- Course manual
- Course videos and checklists
- A 30-minute session with h instruct ors
- Access to a dedicated Slack channel
- 30+ guided exercises

Lab and Exam:

- 60 days of browser-based lab access
- One exam attempt for the Certified DevSecOps Expert (CDE) Certification

WHAT YOU'LL LEARN

- Create a culture of sharing and collaboration among the stakeholders
- Scale the 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

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 LIMITED

COURSE SUBJECTS

Overview of DevSecOps

- 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
- Overview of the DevSecOps critical toolchain
- Repository management tools
- Continuous Integration and Continuous Deployment tools
- Infrastructure as Code (IaC) tools
- Communication and sharing tools
- Security as Code (SaC) tools
- Overview of secure SDLC and CI/CD
- Review of security activities in secure SDLC
- Continuous Integration and Continuous Deployment
- How to move from DevSecOps Maturity Model (DSOMM) Level 2 to Level 4
- Best practices and considerations for Maturity Level 3
- Best practices and considerations for Maturity Level 4
- Security automation and its limits
- DSOMM level 3 and level 4 challenges and solutions

Lumify Work

Customized 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.

Securit y Requirement s and Threat Modelling (TM)

- **What is Threat Modelling?**
- ST RIDE vs DREAD approaches
- Threat modelling and its challenges
- Classical threat modelling tools and how they fit in CI/CD pipeline
- Hands-on Lab: Automate security requirements as code
- Hands-on Lab: using ThreatSpec to do Threat Modelling as Code

- Hands-on Lab: using BDD security to codify threats

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

- Why pre-commit hooks are not a good fit in DevSecOps
- Writing custom rules to weed out false positives and improve the quality of the results
- Various approaches to write custom rules in free and paid tools
- Regular expressions
- Abstract Syntax Trees
- Graphs (Data and Control Flow analysis)
- Hands-on Lab: Writing custom checks in the bandit for your enterprise applications

Advanced Dynamic Analysis (DAST) in CI/CD Pipeline

- Embedding DAST tools into the pipeline
- Leveraging QA/Performance automation to drive DAST scans
- Using Swagger (OpenAPI) and ZAP to scan APIs iteratively. Ways to handle custom authentications for ZAP Scanner
- Using Zest Language to provide better coverage for DAST scans
- Hands-on Lab: using ZAP, Selenium, and Zest to configure in-depth scans
- Hands-on Lab: using Burp Suite Pro to configure per commit/weekly/monthly scans

Note: Students need to bring their Burp Suite Pro License to use in CI/CD

Runtime Analysis (RASP/IAST) in CI/CD Pipeline

- What is Runtime Analysis Application Security Testing?
- Differences between RASP and IAST
- Runtime Analysis and Challenges
- RASP/IAST and its suitability in the CI/CD pipeline
- Hands-on Lab: A commercial implementation of the IAST tool

Infrastructure ure as Code (IaC) and Its Security

- Configuration management (Ansible) security
- Users/Privileges/Keys – Ansible Vault vs Tower
- Challenges with Ansible Vault in CI/CD pipeline
- Introduction to Packer
- Benefits of Packer
- Templates, builders, provisioners, and post-processors
- Packer for continuous security in DevOps Pipelines
- Tools and Services for practicing IaaC (Packer, Ansible, and Docker)
- Hands-on Lab: Using Ansible to harden on-prem/cloud machines for PCI DSS
- Hands-on Lab: Create hardened Golden images using Packer and Ansible

Container (Docker) Security

- What is Docker?
- Docker vs Vagrant
- Basics of Docker and its challenges
- Vulnerabilities in images (Public and Private)
- Denial of service attacks
- Privilege Escalation Methods in Docker
- Security misconfigurations
- Container Security
- Content Trust and Integrity checks
- Capabilities and namespaces in Docker
- Segregating Networks
- Kernel Hardening using SecComp and AppArmor
- Static Analysis of container (Docker) images
- Dynamic Analysis of container hosts and daemons
- Hands-on Lab: Scanning docker images using Clair and its APIs
- Hands-on Lab: Auditing Docker daemon and host for security issues

Secrets Management on Mutable and Immutable Infrast Structure

- Managing secrets in traditional infrastructure
- Managing secrets in containers at Scale
- Secret Management in Cloud
- Version Control Systems and Secrets
- Environment Variables and Configuration files
- Docker, Immutable systems and its security challenges
- Secrets management with Hashicorp Vault and Consul
- Hands-on Lab: Securely store Encryption keys and other secrets using Vault/Consul

Advanced Vulnerability Management

- Approaches to manage the vulnerabilities in the organization
- False positives and
- False Negatives
- Culture and Vulnerability Management
- Creating different metrics for CXOs, devs and security teams Hands-on Lab: Using Defect Dojo for vulnerability management

WHO IS THE COURSE FOR?
This 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

Course participants must have the Certified DevSecOps Professional (CDP) certification. They should also have a basic understanding of application security practices like SAST, DAST, etc.

The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the cours e is conditional on acceptance of these terms and conditions .

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

- 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 Expert](#) [pdf] User Guide
Self Paced Practical DevSecOps Expert, Paced Practical DevSecOps Expert, Practical DevSecOps Expert, DevSecOps Expert, Expert

References

- ✱ [Lumify Work | Lumify Work AU](#)
- ✱ [Lumify Work | Lumify Work AU](#)
- ✱ [Practical DevSecOps Professional - Self-paced | Lumify Work AU](#)
- [User Manual](#)