# Practical DevSecOps

# DevSecOps Professional

**COURSE**

# DevSecOps Professional



**Practical DevSecOps**

Practical DevSecOps is the world's first dedicated DevSecOps certification program.

## ✅ Course Objective

We all have heard about DevSecOps, Shifting Left, Rugged DevOps but there are no clear examples or frameworks available for security professionals to implement in their organization. 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, Etsy handle security at scale and what we can learn from them to mature o ur 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 the DevOps, DevSecOps and move towards advanced concepts such as Security as Code, Compliance as Code, Configuration management, Infrastructure as code, etc.

## ✅ Course Syllabus

The CDP course takes you through the series of stages and maturity levels to mature an organization into a DevSecOps shop. We will cover the following topics as part of the course.

1. Introduction to DevOps and DevSecOps
2. Introduction to the Tools of the trade
3. Secure SDLC and CI/CD pipeline
4. Software Component Analysis (SCA)
5. Static Analysis(SAST) in CI/CD pipeline.
6. Dynamic Analysis(DAST) in CI/CD pipeline.
7. Infrastructure as Code and its security.
8. Compliance as code
9. Vulnerability Management with custom tools

## ✅ Who should take this course?

This course is aimed at anyone who is looking to embed security as part of agile/cloud/DevOps environments like Security Professionals, Penetration Testers, IT managers, Developers and DevOps Engineers

## ✅ Training Duration

The participant can complete the course in 36 hours. That includes 4 hours of video lectures and 32 hours of hands-on practice. However, a participant has lifetime access to the on-demand course with 60 days of online lab access.

# DevSecOps Professional

Practical DevSecOps is the world's first dedicated DevSecOps certification program.

## ✅ What Will Students Learn?

- Gain a solid foundation of the CI/CD pipelines, DevOps, and Secure SDLC.
- Understand the critical parts of DevSecOps processes, tools, and techniques.
- Learn to create a culture of sharing and collaboration among various stakeholders, and departments in an organization.
- Create and maintain DevSecOps Pipelines using SCA, SAST, DAST, IaC, CaC, and Security as code best practices.
- Hardening and compliance of infrastructure according to the organization's policies.
- Learn to consolidate and centrally manage security results from multiple automations and tooling from a CI/CD pipeline.
- Plan and mature an organizations DevSecOps program using industry best practices.

## ✅ Software and Hardware Requirements

Our state of the art DevSecOps Training Platform works within your browser. You can even do the labs from your mobile devices like iPad and Android phones.

Learn DevSecOps in real infrastructure. No installation or configuration is required.

## ✅ What Will Students be Provided?

Resources for your DevSecOps Professional Learning

1. Course Videos and Checklists
2. Course Manual
3. 60 days Online Lab Access
4. 100+ Guided Exercises
5. Access to a dedicated Mattermost channel
6. One exam attempt for Certified DevSecOps Professional Certification

## ✅ Student Prerequisites

1. Course participants should have knowledge of running basic Linux commands like ls, cd, mkdir etc.
2. Course participants should have a basic understanding of application Security practices like OWASP Top 10.
3. You don't need any experience with DevOps tools.

### *Learn more*

To learn more about our courses, certifications and pricing, please visit **our courses** or **contact us**

# DevSecOps Professional

Practical DevSecOps is the world's first dedicated DevSecOps certification program.

✓ **How much time should I be spending in the course?**

It's very difficult to zero in on the exact time commitment it all depends on how comfortable you are with the technology, ability to find answers on Google, etc., However, we have created a rough breakdown below.

✓ **Breakdown by DevSecOps Expertise**

Total hours you need to spend on the course, if you wish to explore some topics in depth, you would need to plan for extra time.

| Module Name | Beginner | Intermediate | Expert |
|---|---|---|---|
| 1. Introduction to DevSecOps | 1 | 1 | 1 |
| 2. DevSecOps Tools of the trade | 3 | 2 | 2 |
| 3. Secure SDLC and CI/CD | 4 | 3 | 2 |
| 4. Software Component Analysis | 5 | 4 | 3 |
| 5. SAST (Static Analysis) | 5 | 4 | 3 |
| 6. DAST (Dynamic Analysis) | 5 | 4 | 3 |
| 7. Infrastructure as Code | 5 | 4 | 3 |
| 8. Compliance as code | 5 | 4 | 3 |
| 9. Vulnerability Management | 3 | 2 | 1 |
| **Hours spent** | **36** | **28** | **20** |

# DevSecOps Professional

**Detailed Syllabus**



## DAY 1

### 1 Introduction to DevOps and DevSecOps

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

### 2 Introduction to the Tools of the trade

1. Github/Gitlab/BitBucket
2. Docker
3. Docker Registry
4. Ansible
5. Jenkins/Travis/Gitlab CI/Bitbucket
6. Gauntlt
7. Inspec
8. Bandit/retireJS/Nmap
9. **Hands-On Labs**: Use Vagrant to practice Infrastructure as a Code
10. **Hands-On Labs**: Building a CI Pipeline using Jenkins/Travis and GitHub/bitbucket.
11. **Hands-On Labs**: Use the above tools to create a complete CI/CD pipeline.

# DevSecOps Professional

**Detailed Syllabus**

**3** **Secure SDLC and CI/CD pipeline**

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

# DevSecOps Professional

## Detailed Syllabus

### 4 Software Component Analysis(CSA) in CI/CD pipeline

1. What is Software Component Analysis?
2. Software Component Analysis and its challenges.
3. What to look in an SCA solution (Free or Commercial).
4. Embed SCA tools like OWASP Dependency Checker, Safety, Retirejs, NPM Audit, Synk into Pipeline.
5. **Demo**: OWASP Dependency Checker to scan third party component vulnerabilities in Java Code Base.
6. **Hands-On Labs**: RetireJS and NPM to scan third party component vulnerabilities in JS Code.
7. **Hands-On Labs**: using Safety/pip to scan third party component vulnerabilities in Python Code Base.

### 5 SAST (Static Analysis) in CI/CD pipeline

1. What is Static Application Security Testing?
2. Static Analysis and its challenges.
3. Embedding SAST tools into the pipeline.
4. Secrets scanning to prevent secret exposure in the code.
5. Writing custom checks to catch secrets leakage in an organization.
6. **Hands-On Labs**: using SpotBugs to scan Java code.
7. **Hands-On Labs**: using Trufflehog/Gitrob to scan for secrets in CI/CD pipeline.
8. **Hands-On Labs**: using brakeman/bandit to scan Ruby on Rails and Python Code Base.

### 6 DAST (Dynamic Analysis) in CI/CD pipeline

1. What is Dynamic Application Security Testing?
2. Dynamic Analysis and Its challenges ( Session Management, AJAX Crawling )
3. Embedding DAST tools like ZAP and Burp Suite into the pipeline.
4. SSL misconfiguration testing
5. Server Misconfiguration Testing like secret folders and files.
6. Sqlmap testing for SQL Injection vulnerabilities.
7. **Hands-On Labs**: using ZAP to configure per commit/weekly/monthly scans.
8. **Demo**: using Burp Suite to configure per commit/weekly/monthly scans.

# DevSecOps Professional



**Practical DevSecOps**

## Detailed Syllabus

### 7  Infrastructure as Code and Its Security

1. What is Infrastructure as Code and its benefits?
2. Platform + Infrastructure Definition + Configuration Management.
3. Introduction to Ansible.
   - a. Benefits of Ansible.
   - b. Push and Pull based configuration management systems
   - c. Modules, tasks, roles, and Playbooks
4. Tools and Services which helps to achieve IaaC
5. **Hands-On Labs**: Vagrant, Docker, and Ansible
6. **Hands-On Labs**: Using Ansible to create Golden images and harden Infrastructure.

### 8  Compliance as code

1. Different approaches to handle compliance requirements at DevOps scale
2. Using configuration management to achieve compliance.
3. Manage compliance using Inspec/OpenScap at Scale.
4. **Hands-On Labs**: Create an Inspec profile to create compliance checks for your organization
5. **Hands-On Labs**: Use Inspec profile to scale compliance.

### 9  Vulnerability Management with custom tools

1. Approaches to manage the vulnerabilities in the organization.
2. **Hands-On Labs**: Using Defect Dojo for vulnerability management.

# DevSecOps Professional

## Certification Process

### ✓ Exam and certification process

Our certifications are well recognized in the industry as we ensure our students gain practical skills to implement DevSecOps. To ensure we deliver on our promise, we have a rigorous certification program.

**CDP exam** is an online, task-oriented exam where you attempt to solve **5 challenges** (tasks) in a span of **12 hours**. The exam is based on the content covered in the course but might require further research to pass the exam. Once the exam is done, you have **24 hours** to send us the exam report.

> *Please note*
> it's not an MCQ or tests your memory type of exam but practical applicability of the content covered in the course.

### ✓ Exam Pass percentage

The student needs to achieve at least 80 points (80%) to achieve the CDP certification.

### ✓ Exam Challenges/tasks

The exam has 5 challenges for the exam, each of these challenges provides you points based on how complete or partial your solution was. You would need to score 80 points out of 100 (80%) to achieve the CDP certification.

### ✓ Exam documentation

After the exam, you have about 24 hours to send us the exam report on our email.

### ✓ Steps Involved

A typical certification flow involves 5 steps.

1. The student schedules the exam.

2. The student will receive an exam guide that includes challenges via email. Our instructors will be there to assist you if you face any difficulty while connecting to the exam lab.

3. The student will connect to the exam lab using details from the exam guide and will attempt the practical exam.

4. After the exam, the student will have 24 hours to send us the exam report.

5. Practical DevSecOps team will evaluate the report and share the result (pass/fail) with the student.

# Practical DevSecOps

## About us

Practical DevSecOps (a Hysn Technologies Inc company) offers vendor-neutral, practical, and hands-on DevSecOps training and certification programs for IT Professionals. Our online training and certifications are focused on modern areas of information security, including DevOps Security, Cloud-Native Security, Cloud Security & Container security. The certifications are achieved after rigorous tests (12-24 hour exams) of skill and are considered the most valuable in the information security field.

[f] @pdevsecops

[t] @pdevsecops

[in] Practical DevSecOps

**USA**

+1 (415) 800 4768
trainings@practical-devsecops.com
201 Spear St #1100, San Francisco, CA 94105

**India**

+91 81216 77008
apac@practical-devsecops.com
Hyderabad, India

**Singapore**

+65 85042132
apac@practical-devsecops.com
531A Upper Cross Street #04-95
Hong Lim Complex Singapore 051531

Practical
DevSecOps