Practical DevSecOps

DevSecOps Expert

COURSE

www.practical-devsecops.com

DevSecOps Expert

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 our security programs.

In our advanced DevSecOps Expert course, 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 Threat Modelling as Code, RASP/IAST, Container Security, Secrets management, etc.

Course Syllabus

The CDE 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. Overview of DevSecOps.
2. Security Requirements and Threat Modelling (TM).
3. Advanceda Static Analysis (SAST) in CI/CD pipeline.
4. Advanced Dynamic Analysis(DASTI in CI/CD pipeline Runtime.
5. Analysis(RASP/IASTI in CI/CD pipeline.
6. Infrastructure as Code(laC) and Its Security.
7. Container (Docker) Security.
8. Secrets management on mutable and immutable Infrastructure.
9. Advanced vulnerability management.

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 Expert

Practical DevSecOps

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

What Will Students Learn?

- Understand, implement and manage advanced DevSecOps programs in an organization
- Master the skills required for secure design assessment and threat modeling
- Write Custom rulesets and reduce false-positive fatigue using automation.
- Write Custom roles for SAST, DAST, OS hardening, and Infrastructure as Code.
- Write Custom rulesets for Product Security tools, like SAST, DAST, RASP.
- Gain the ability to scan, audit, and improve the security of Container (Docker) systems.
- Learn how to manage secrets in traditional and containerized environments.
- Learn and understand performing Vulnerability Management at Scale

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 Expert Learning

1. Course Videos and Checklists
2. Course Manual
3. 60 days Online Lab Access
4. 50+ Guided Exercises
5. Access to a dedicated Mattermost channel
6. 30-Minutes One on One session with Instructor
7. One exam attempt for Certified DevSecOps Expert Certification

Student Prerequisites

1. Course participants must have the Certified DevSecOps Professional (CDP) certification.
2. Course participants should have a basic understanding of Application Security Practices like SAST, DAST, etc.

Learn more

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

DevSecOps Expert

Practical DevSecOps

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. Overview of DevSecOps	1	1	1
2. Security Requirements & TM	3	2	2
3. Advanced SAST	4	3	2
4. Advanced DAST	5	4	3
5. RASP/IAST in CI/CD pipelines	5	4	3
6. IaC and its security	5	4	3
7. Container (Docker) Security	5	4	3
8. Secrets management	5	4	3
9. Vulnerability Management	3	2	1
Hours spent	**36**	**28**	**20**

DevSecOps Expert

Practical DevSecOps

Detailed Syllabus

DAY 1

1 Introduction to DevOps and DevSecOps

1. DevOps Building Blocks- People, Process and Technology.
2. DevOps Principles - Culture, Automation, Measurement and Sharing (CAMS)
3. Benefits of DevOps - Speed, Reliability, Availability, Scalability, Automation, Cost and Visibility.
4. Overview of the DevSecOps critical toolchain.
    a. Repository management tools.
    b. Continuous Integration and Continuous Deployment tools.
    c. Infrastructure as Code (IaC) tools.
    d. Communication and sharing tools.
    e. Security as Code (SaC) tools.
5. Overview of secure SDLC and CI/CD
    a. Review of security activities in secure SDLC.
    b. Continuous Integration and Continuous Deployment.
6. How to move from DevSecOps Maturity Model (DSOMM) Level 2 to Level 4.
    a. Best practices and considerations for Maturity Level 3.
    b. Best practices and considerations for Maturity Level 4.
    c. Security automation and its limits.
    d. DSOMM level 3 and level 4 challenges and solutions.

2 Security Requirements and Threat Modelling (TM)

1. What is Threat Modelling?
2. STRIDE vs DREAD approaches
3. Threat modelling and its challenges.
4. Classical Threat modelling tools and how they fit in CI/CD pipeline
5. **Hands-On Labs**: Automate security requirements as code.
6. **Hands-On Labs**: using ThreatSpec to do Threat Modelling as Code.
7. **Hands-On Labs**: using BDD security to codify threats.

DevSecOps Expert

Practical DevSecOps

Detailed Syllabus

3 Advanced Static Analysis(SAST) in CI/CD pipeline

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

DAY 2

4 Advanced Dynamic Analysis(DAST) in CI/CD pipeline

1. Embedding DAST tools into the pipeline.
2. Leveraging QA/Performance automation to drive DAST scans.
3. Using Swagger (OpenAPI) and ZAP to scan APIs iteratively.
4. Ways to handle custom authentications for ZAP Scanner.
5. Using Zest Language to provide better coverage for DAST scans.
6. **Hands-On Labs**: using ZAP + Selenium + Zest to configure in-depth scans
7. **Hands-On Labs**: using Burp Suite Pro to configure per commit/weekly/monthly scans.

Please note

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

5 Runtime Analysis(RASP/IAST) in CI/CD pipeline

1. What is Runtime Analysis Application Security Testing?.
2. Differences between RASP and IAST.
3. Runtime Analysis and challenges.
4. RASP/IAST and its suitability in CI/CD pipeline.
5. **Hands-On Labs**: A commercial implementation of the IAST tool.

DevSecOps Expert

Practical DevSecOps

Detailed Syllabus

6 Infrastructure as Code (IaC) and Its Security

1. Configuration management (Ansible) security
    a. Users/Privileges/Keys - Ansible Vault vs Tower.
    b. Challenges with Ansible Vault in CI/CD pipeline.
2. Introduction to Packer
    a. Benefits of Packer.
    b. Templates, builders, provisioners, and post processors.
    c. Packer for continuous security in DevOps Pipelines.
3. Tools and Services for practising IaaC (Packer + Ansible + Docker).
4. **Hands-On Labs**: Using Ansible to harden on-prem/cloud machines for PCIDSS.
5. **Hands-On Labs**: Create hardened Golden images using Packer + Ansible

DAY 3

7 Container (Docker) Security

1. What is Docker
2. Docker vs Vagrant
3. Basics of Docker and its challenges
    a. Vulnerabilities in images (Public and Private)
    b. Denial of service attacks
    c. Privilege escalation methods in Docker
    d. Security misconfigurations.
4. Container Security
    a. Content Trust and Integrity checks
    b. Capabilities and namespaces in Docker
    c. Segregating Networks
    d. Kernel Hardening using SecComp and AppArmor.
5. Static Analysis of container(Docker) images.
6. Dynamic Analysis of container hosts and daemons.
7. **Hands-On Labs**: Scanning docker images using Clair and its APIs.
8. **Hands-On Labs**: Auditing Docker daemon and host for security issues.

DevSecOps Expert

Practical DevSecOps

Detailed Syllabus

8 Secrets management on mutable and immutable infrastructure

1. Managing secrets in traditional infrastructure.
2. Managing secrets in containers at Scale.
3. Secret Management in Cloud.
    a. Version Control systems and Secrets.
    b. Environment Variables and Configuration files.
    c. Docker, Immutable systems and its security challenges.
    d. Secrets management with Hashicorp Vault and consul.
4. **Hands-On Labs**: Securely store Encryption keys and other secrets using Vault/Consul.

9 Advanced Vulnerability Management

1. Approaches to manage the vulnerabilities in the organization.
2. False positives and False Negatives.
3. Culture and Vulnerability Management.
4. Creating different metrics for CXOs, devs and security teams.
5. **Hands-On Labs**: Using Defect Dojo for vulnerability management.

DevSecOps Expert

Practical DevSecOps

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.

CDE exam is an online, task-oriented exam where you attempt to solve **5 challenges** (tasks) in a span of **24 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 70 points (70%) to achieve the CDE 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 70 points out of 100 (70%) to achieve the CDE 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 the above details and attempts the 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.

@pdevsecops

@pdevsecops

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