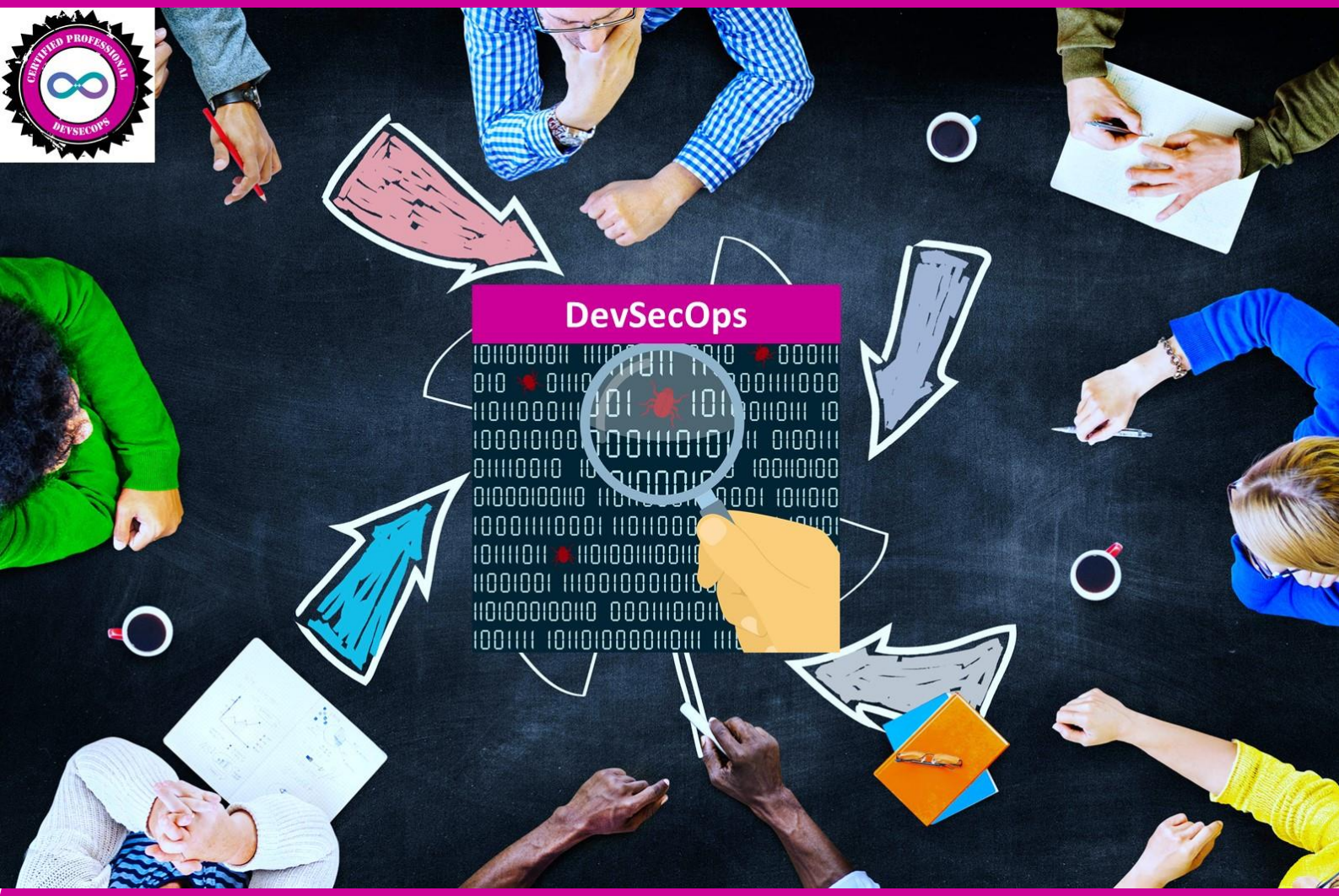
Certified Professional DevSecOps Certification Course



http://cpdevsecops.devopsppalliance.org/
http://devopsppalliance.org/cp-devsecops.html

info@devopsppalliance.org

/devopspp

http://devopsppalliance.org/

What is CP-DevSecOps course?

The course is designed to practically learn and implement continuous Security in the DevOps lifecycle (**DevSecOps**) using open source tools. The program is relevant for anyone on the DevOps team who would like to learn the practical aspects of Continuous Security in DevOps cycle.

CP- DevSecOps certification exam can be taken by anyone with or without going through the training program covering the learning objectives below. CP-DevSecOps certification exam is the only globally accepted certification exam covering practical assessment for the DevOps Security (**DevSecOps**). CP-DevSecOps learning objective gives the coverage topics for anyone who want to give the exam. Any training covering the CP-DevSecOps Syllabus would be covering the learning objectives in a practical manner.

The training course provided by accredited CP-DSC license trainers is applicable for all roles in the DevOps and Agile World. Knowledge, experience & certification is consciously designed to focus on "practical aspects of DevOps Security" and **not** just on "theory".

How is CP-DevSecOps useful?

With the growth of Cloud, Microservices architecture, use of Open Source tools & Agile methodology, risk of security breaches, cyber attack, ransomware attack has increased multi-fold. DevSecOps market size which is valued at USD 4.4 billion in 2022 expected to grow to USD 32 billion by 2032.

CP-DevSecOps is designed to train software professionals with the concepts of implementing Security in every stage of software development.

The training provided by accredited license trainers is completely hands-on covering installation, creation of security testing scripts, automating scans etc. using the features of **"Tools of Trade"** with ample time given to practice until the concepts are mastered.

This syllabus and hence the training course focus on the most relevant areas for implementing Security such as Cloud, Container, Application, Infrastructure, Supply chain etc. in the DevOps scenario using tools like **Vault**, **ZAP, Burp, Arachni, Gauntlt, Gauntlt-Docker, Snyk, Cloud (AWS/GCP/Azure)**.

Am I Eligible?

Anyone having basic experience in Software Development & Testing can go for this certification. It is recommended that participants understand the basics of Agile and DevOps. This program is focussed on the DevOps Security and will not cover the basics of Agile and DevOps.

What is the Training and Certification Exam structure?

CP-DevSecOps is designed specifically for corporates and working professionals alike. It is a **4 full days** course followed by an examination. **Certification Examination can be taken within 15 working days of the completion of the training**.

CP-DevSecOps certification exam has two parts. A theory exam which is of 1 hour duration and is conducted through online multiple choice question pattern. The theory exam is of 40 marks with no negative marking. The practical exam is taken immediately after the theory exam and is of 2-hour duration. The practical exam is case study based and follows the pattern taught in the program.

Table of Contents

What is CP-DevSecOps course? 2
How is CP-DevSecOps useful? 2
Am I Eligible? 2
What is the Training and Certification Exam structure? 3
1. Thinking Of DevSecOps 5
1.1 DevSecOps Overview 5
1.2 Secure Software Development Lifecycle (SDLC) 5
2. Implementing DevSecOps 5
2.1 Plan & Design 5
2.2 Develop/Code 6
2.3 Build 6
2.4 Test 6
2.5 Deploy 6
2.6 Operate and Monitor 6
2.7 Security of CICD 6
2.8 DevSecOps Best Practices and Case Studies 7
3. Labs 7
3.1 Setting up a Secure CI/CD Pipeline 7
3.2 Secrets Management 7
3.3 Cloud Security 7
3.4 Container Security 7
3.5 Securing Infrastructure as Code 7
How do I enroll myself? 7

1. Thinking Of DevSecOps

1.1 DevSecOps Overview

- History Of DevSecOps
- DevOps Vs DevSecOps/DevSecOps Vs SRE Vs Agile/DevSecOps Vs SecDevOps
- What is DevSecOps?
- Why is DevSecOps important?
- Benefits of implementing DevSecOps / Advantages of DevSecOps
- How do we achieve these benefits?
- Myths
- Challenges
- Who is DevSecOps Engineers
- DevSecOps Engineers Skills
- DevSecOps Engineers Roles & Responsibilities
- How to become DevSecOps Engineer
- What Does DevSecOps Engineer Do?
- Challenges Faced by DevSecOps Engineers
- Learning Resources, Tools, Technologies for DevSecOps Engineers

-

1.2 Secure Software Development Lifecycle (SDLC)

- Overview of the SDLC
- Secure SDLC
- Integrating security into each phase of the SDLC
- The DevSecOps Lifecycle
- DevSecOps Manifesto
- OWSAP Top 10 & DevSecOps

2. Implementing DevSecOps

2.1 Plan & Design

- Plan for collaboration between Development, Security & Operation
- Shift Left Security
- Plan Security Training
- Secure Development Framework/Lifecycle/Practices
- Bridging Security to Speed of DevOps
- Introduction to Threat Modelling
- Planning Various Security Approach
    - Secrets Management
    - Application Security
    - API Security
    - Cloud Security
    - Cloud Native Security
    - Infrastructure as Code (IaC) Security
    - Container Security
    - Supply Chain Security

    - Open Source Security (OSS)
    - Mobile Security
    - Ethical Hacking
    - Cybersecurity
- Governance

2.2 Develop/Code

- Best practices for secure coding
- Repository access control
- Developing Various Security Approach
- Automation approach to DevSecOps
    - Security as Code
    - Policy as Code
    - Compliance as Code
    - Infrastructure as Code

2.3 Build

- SAST(Static Application Security Testing)
- Interactive Application Security Testing (IAST)
- Introduction to Software Composition Analysis (SCA)

2.4 Test

- Overview of application security testing
- Introduction to Static Application Security Testing (SAST)
- Introduction to Dynamic Application Security Testing (DAST)
- DAST for your Web Application
- Penetration Testing

2.5 Deploy

- Security Hardening & Config
- Security Scanning

2.6 Operate and Monitor

- Security Monitoring and Incident Response
- Implementing security monitoring in DevSecOps
- Incident Management in a DevSecOps environment
- Run-time Application Security Protection (RASP)
- Security Analysis, Patch, Monitor, Audit
- Introduction to Bug Bounty Programs

2.7 Security of CICD

- Introduction to CI/CD pipelines
- Implementing security checks in CI/CD pipelines
- Introduction to Vulnerability Management
- Automating security testing and vulnerability scanning

2.8 DevSecOps Best Practices and Case Studies

- Industry best practices for DevSecOps
- Case studies of successful DevSecOps implementations
- Lessons learned and recommendations
- How to implement DevSecOps
- 15 top DevSecOps Worst Practices

3. Labs

3.1 Setting up a Secure CI/CD Pipeline

- Configuring a CI/CD pipeline with security checks
- Automated SAST in CI/CD Pipeline
- Automated DAST in CICD Pipeline using OWASP ZAP
- Integrating vulnerability scanning tools

3.2 Secrets Management

- Git Secrets
- Static and Dynamic Secrets Management in Kubernetes
- Secrets Management with Azure Key Vault

3.3 Cloud Security

- Secure your AWS S3 Bucket
- Effective Creation and Deployment of AWS IAM Policies
- AWS Threat Detection and Monitoring

3.4 Container Security

- Secure Container Images in CI/CD
- Scanning container images for vulnerabilities
- Implementing runtime security measures for containers
- Runtime Container Security on Kubernetes

3.5 Securing Infrastructure as Code

- Implementing security controls in cloud environments
- Automating security checks for infrastructure code

How do I enroll myself?

You can send us an email for your training and certification needs.

If you are interested in getting a corporate program done at your location please do get in touch with us on ATASupport@AgileTestingAlliance.org