Practical DevSecOps

Certified Security Champion

COURSE

www.practical-devsecops.com

Certified Security Champion

Practical DevSecOps

Unlock the key to building secure & Trustworthy applications.

Abstract

The Certified Security Champion course provides engineers with practical hands-on knowledge to help them in building more secure web applications. Students will learn to develop trustworthy web applications while avoiding common security pitfalls, using best practices and industry frameworks.

Cybersecurity is a wide-ranging topic that covers many areas including but not limited to cryptography, penetration testing, security testing in the software development life cycle, wireless security, denial of service attacks, threats, and vulnerabilities. This course focuses on secure application development with an emphasis on web-related security issues. A review of the OWASP Top 10 list is included.

In this intensive course, you'll learn how to discover and fix vulnerabilities in application code. Throughout the course, students will be exposed to a wide variety of security topics, including SQL Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), XML External Entity Attacks (XXE), Cross-Site Request Forgery (CSRF), Open Redirects and many more. The course also focuses on various areas of infrastructure security, risk management, threat modelling, and agile collaboration techniques.

By the end of this course, you will develop practical security knowledge, that you can immediately begin applying at work.

Certified Security Champions can cut the cost of security vulnerability remediation by half and reduce time spent remediating vulnerabilities by 75%. By taking this course, learners are guaranteed to increase their organization's security effectiveness.

The Certified Security Champions course is a must-take for everyone involved in web development. From Front-end developers to security auditors, this course will give you the knowledge and hands-on material you need to build more secure Web Applications. Dev and Sec folks are working more closely together than ever before, and this course will put everyone on the same page.

Certified Security Champion

Practical DevSecOps

Unlock the key to building secure & Trustworthy applications.

Learning Objectives

The students will be provided with

1. Building solid foundations that are required to understand the application security landscape
2. Building foundational knowledge required to work with infrastructure security
3. Understanding the wide range of skills and abilities that are required to be a security champion
4. Embedding security while creating, running, and maintaining modern applications
5. Gaining abilities to apply practical application security skills in a real-world environment
6. Gaining skills and knowledge to liaise with security and other departments to make everyone responsible for the security
7. Gaining analytical abilities to observe and advise various security controls, and solutions to secure DevOps
8. Understanding the fundamentals of assessing and managing risks

Prerequisites

1. Understanding of developing or testing web applications
2. Foundational knowledge of software development life cycle

Course Duration

1. **2 Days** - Instructor-Led Training
2. **36 hours** - Self Paced Training

Skill Level

1. Beginner
2. Intermediate

Target Audience

1. Security Champions
2. Developers
3. QA Engineers
4. DevOps
5. Junior AppSec Engineers

Learn more

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

Certified Security Champion

Practical DevSecOps

Detailed Syllabus

DAY 1

1 Module 0: Introduction to the course

1. Course Introduction (About the course, syllabus, and how to approach it)
2. About Certification and how to approach it
3. Lab Environment
4. Course support (Mattermost)
5. Security Champion 101
6. Security Champion's History and Beyond

2 Module 1: AppSec Basics

1. Introduction to Application Security
2. HTTP Security Basics
3. Introduction to Burp Suite
4. OWASP Top 10 Basics
   a. Injection (SQL and other injections)
   b. Cross-Site Scripting (XSS)
   c. Cross-Site Request Forgery (CSRF) and SSRF
   d. Broken Authentication and Session Management
   e. XML External Entities (XXE)
   f. Insecure Direct Object Reference (IDOR)
   g. Security Misconfiguration
   h. Unvalidated Requests and Forwards
5. **Hands-On Labs:** SQL Injection
6. **Hands-On Labs:** XSS and CSRF
7. **Hands-On Labs:** SSRF
8. **Hands-On Labs:** Local File Inclusion (LFI) and File Upload issues

Certified Security Champion

Practical DevSecOps

Detailed Syllabus

3 Module 2: Secure Code Review

1. What is Secure Code Review?
2. How to approach Secure code review
3. Tools of the trade
4. Reviewing the code from a security perspective
    a. Input and output validation
    b. Authentication issues
    c. Authorization issues
    d. Security Misconfigurations
5. **Hands-On Labs:** Input validation using industry best practices
6. **Hands-On Labs:** Output encoding to prevent client-side attacks like XSS
7. **Hands-On Labs:** Bruteforce attacks and secret questions
8. **Hands-On Labs:** Information leakage with password reset workflows
9. **Hands-On Labs:** Best practices in implementing role-based access control
10. **Hands-On Labs:** Risks with unvalidated redirects and forwards

DAY 2

4 Module 3: Primer on Risk Management

1. Introduction to Risk management
2. Risk Assessment
3. Risk Calculation
4. Risk Treatment
    a. How to mitigate risks
    b. How to avoid risks
    c. How to transfer risks
    d. How to accept risks
5. Plan, design, and implement a risk-management process
6. Understand the current threat landscape
7. Continuously improve security systems to reduce risk exposure
8. Ensure business continuity while reducing the risks to the organization

Certified Security Champion

Practical DevSecOps

Detailed Syllabus

5 Module 4: Threat Modeling

1. What is Threat Modelling?
2. Risk Management vs. Threat modeling
3. STRIDE vs. DREAD approaches
4. Threat Modeling Process and its challenges
    a. Decompose the application
    b. Identify the Threats
    c. Document and rate the threats, and risks
    d. Design and create defenses
5. Classical Threat modeling tools and how they fit in CI/CD pipeline
6. **Hands-On Labs:** Automate security requirements as code
7. **Hands-On Labs:** Using ThreatSpec to achieve Threat Modelling as Code

6 Module 5: DevSecOps Basics

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. Common Challenges faced when using the DevOps principles
6. Secure SDLC
    a. Overview of secure SDLC and CI/CD
    b. Review of security activities in secure SDLC
    c. Continuous Integration and Continuous Deployment
7. **Hands-On Labs:** How to embed SCA tool into CI/CD pipeline
8. **Hands-On Labs:** How to embed SAST tool into CI/CD pipeline

Certified Security Champion

Practical DevSecOps

Detailed Syllabus

DAY 3

7 Module 6: Infrastructure as Code and Its Security

1. Infrastructure as Code and its benefits
2. Platform + Infrastructure Definition + Configuration Management
3. Introduction to Ansible
4. Benefits of Ansible
5. Push and Pull based configuration management systems
6. Modules, tasks, roles, and Playbooks
7. Tools and Services that help to achieve IaC
8. **Hands-On Labs:** Docker and Ansible
9. **Hands-On Labs:** Using Ansible to create Golden images and harden Infrastructure

8 Module 7: Agile Communications, Collaboration, and Soft Skills

1. The need for Agile communication and collaboration
2. How to handle conflicting priorities among teams
3. How to work security teams to find common ground
4. Holding people accountable for security
5. Staying empathetic and assertive
6. Plan, design, and implement processes to resolve any issues among the teams

Certified Security Champion

Practical DevSecOps

Certification Process

Exam and certification process

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

CSC exam is an online, task-oriented exam where you attempt to solve five challenges (tasks) in **6 hours**. The exam is based on the content covered in the course but might require further research to pass the exam. After the exam, 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 CSC certification.

Exam Challenges/tasks

The exam has five 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 CSC certification.

Exam documentation

After the exam, you have about 24 hours to send us the exam report via 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