Practical DevSecOps

Cloud-Native Security Expert

COURSE

www.practical-devsecops.com

Cloud-Native Security Expert

Practical approach to Offensive And Defensive techniques in Cloud Native technology

✓ Course Objective

Cloud-Native technologies like Microservices, containers, and Kubernetes have emerged as the go-to way to create, deploy and manage microservices for both on-prem and cloud environments. Cloud-Native technologies bring a wealth of benefits; however, The task of securing your cloud-native environment is daunting.

The **Certified Cloud-Native Security Expert (CCNSE)** is a vendor-neutral course and certification program that is designed to assess the level of security knowledge a candidate has on Cloud Native Technologies like Microservices, APIs, and Kubernetes.

The course is designed to give students a practical view of Kubernetes security, covering not only the theory but immediately applicable tools and techniques. The course is project-oriented, with 60+ hands-on labs that will put your newly gained knowledge into action and guide you along the way.

✓ Who should take this course?

This course is aimed at professionals interested in securing container and kubernetes environments as part of agile/cloud/DevOps transformations like Security Professionals, Penetration Testers, Red Teamers, Application Security Engineers, IT managers, Developers, and DevOps Engineers.

✓ Learning Objectives

The following are the course's objectives.

1. Build a solid foundation that is required to understand the container and k8s security landscape
2. Gain the necessary skills to analyze, assess, evaluate, and secure applications; APIs and microservices; containers; and Kubernetes
3. Gain a practical understanding of how to hack misconfigured Kubernetes workloads
4. Learn and implement different ways of Authentication and Authorization methods used in Kubernetes
5. Learn how different Admission controllers help apply defense in depth to regulate and audit workloads in a Kubernetes Cluster
6. Learn, apply and practice different techniques to manage clusterwide data in a distributed setup
7. Practice and implement a myriad of techniques to secure secrets and other sensitive data processed and consumed in a Kubernetes Cluster.
8. Experience Network security and Zero Trust in action using Network policies and Service Meshes.
9. Gain the necessary skills to Defend Kubernetes cluster from most common attacks.

Cloud-Native Security Expert

Practical DevSecOps

Practical approach to Offensive And Defensive techniques in Cloud Native technology

✓ Course Duration

The participant can complete the course in 40 hours. That includes 10 hours of video lectures and 30 hours of hands-on practice. However, a participant has lifetime access to the on-demand course with 60 days of online lab access.

✓ What will students be provided?

The students will be provided with

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

✓ Course Prerequisites

1. Course participants should have knowledge of running basic Linux commands like ls, cd, mkdir, etc.,
2. The course also needs you to know some basic understanding of Container system and technology
3. The course also needs you to know some basic understanding of Kubernetes.
4. Understanding of OWASP Top 10 vulnerabilities is an added advantage.

✓ Course Syllabus

This course is targeted toward individuals or teams interested in devoting their careers to learning and implementing industry security best practices around Cloud Native technologies like containers, Kubernetes and microservices security.

The following topics are covered as part of the course.

1. Introduction to Cloud-Native Concepts and its Security
2. Introduction to Microservices Architecture
3. Containers and Container Security
4. Introduction to Kubernetes
5. Hacking Kubernetes Cluster
6. Kubernetes Authentication and Authorization
7. Kubernetes Admission Controllers
8. Kubernetes Data Security
9. Kubernetes Network Security
10. Defending Kubernetes Cluster

✓ Software and Hardware Requirements

Our state-of-the-art Cloud-Native Security Training Platform works within your browser. All you need is a modern browser on a laptop or desktop.

Learn more

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

Cloud-Native Security Expert

Detailed Syllabus

DAY 1

1 Introduction to Cloud-Native Concepts and its Security

1. Course Introduction (About the course, syllabus, and how to approach it)
2. About Certification and how to approach it
3. Lab Environment
4. Lifetime course support (Mattermost)
5. Overview of the Cloud Native Technologies
6. The 4C's of Cloud-Native Security
    a. Cloud
    b. Clusters
    c. Containers
    d. Code (SCA, SAST, DAST) - DevSecOps
7. Security and Threat Model of Cloud-Native technologies
    a. Overview of Cloud Security
    b. Overview of Container Security (Container Vulnerability, Supply Chain Attack, Least Privilege)
    c. Overview of Kubernetes Security
    d. Overview of Microservices Security
8. **Hands-on Exercise**: Learn how to use our browser-based lab environment

Practical DevSecOps

Cloud-Native Security Expert

Detailed Syllabus

2 Introduction to Microservices Architecture

1. The need for microservices
2. Monolith vs. Microservices
3. Technical and Business pros and cons of Microservices
4. Tools of the trade
    - a. Source code management
    - b. CI/CD tools
    - c. Artefact management
    - d. Cloud Platform
    - e. Infrastructure as code
    - f. Monitoring and logging tools
    - g. Collaboration tools
5. REST APIs
    - a. What is an API
    - b. API Security
    - c. Introduction to OWASP API Top 10
        - i. Software Component Analysis of API
        - ii. Static Application Security Testing of API
        - iii. Dynamic Application Security Testing of API
6. **Hands-on Exercises**:
    - a. Create a simple CI/CD pipeline
    - b. Create advanced CI/CD pipeline
    - c. Continuous Deployment
    - d. Exploiting Containerized Application
    - e. Docker Privilege Escalation
    - f. Hardening container workload (host)

Cloud-Native Security Expert

Detailed Syllabus

3 Containers and Container Security

1. What is a container?
2. Container vs. Virtualization
   a. Container Advantages
   b. Container Disadvantages
3. Docker Architecture and its components
   a. Command Line Interface(CLI)
   b. Engine (Daemon, API)
   c. Runtime (containerd, shim, runc)
4. Basics of container technology and its challenges
5. Container fundamentals
   a. Namespaces
   b. Cgroup
   c. Capabilities
6. Ways to interact with container ecosystem
7. Container security issues
8. Container Defenses
9. **Hands-on Exercises**:
   a. Docker command basics
   b. Docker image
   c. Image-based attacks
   d. Build a secure and miniature docker image
   e. Docker registry
   f. Registry-based attacks
   g. Docker Content Trust
   h. Securing container using seccomp
   i. Securing container using apparmor

Practical DevSecOps

Cloud-Native Security Expert

Detailed Syllabus

DAY 2

4 Introduction to Kubernetes

1. Introduction to Kubernetes
2. Kubernetes use cases
3. Kubernetes Architecture (Core Components)
    a. Cluster, Nodes, and Pods
    b. API Server
    c. Controller Manager
    d. Etcd
    e. kube-scheduler
    f. kubelet
    g. Kube-proxy
    h. Container Runtime
4. Bootstrapping the Kubernetes cluster
5. Kubernetes Package Manager
    a. Understanding Helm Workflow
    b. Creating Helm Charts
6. **Hands-on Exercises**:
    a. Bootstrapping the cluster using kubeadm, kind
    b. Kubernetes basics component
    c. kubectl basics commands
    d. Kubernetes storage
    e. Kubernetes networking

5 Hacking Kubernetes Cluster

1. Kubernetes Attack Surface and Threat Matrix
2. Common Kubernetes security issues
3. Differences in k8s installations (support for PSP vs. no PSP)
4. **Hands-on Exercises**:
    - a. Kubernetes Reconnaissance:
        - i. Port scanning
        - ii. Misconfigured Kubernetes components
        - iii. Access Kubernetes dashboard
    - b. Reconnaissance using kube-hunter
    - c. Exploiting Privileged Containers
    - d. Crashing Kubernetes cluster
    - e. Compromising Kubernetes secrets
    - f. Supply chain attack using the poisoned image and malicious helm charts
    - g. Sniffing Kubernetes Network Traffic

6 Kubernetes Authentication and Authorization

1. Fundamentals of Kubernetes Authentication and Authorization
2. Authentication mechanisms in Kubernetes
    - a. Authentication with Client Certificates
    - b. Authentication with Bearer Tokens
    - c. HTTP Basic Authentication
    - d. Remote Authentication
3. Authorization mechanisms in Kubernetes
    - a. Node Authorization
    - b. Attribute Based Access Control (ABAC)
    - c. Role-Based Access Control (RBAC)
4. **Hands-on Exercises**:
    - a. Kubernetes Authentication using Keycloak
    - b. Find misconfigured RBAC using KubiScan
    - c. Static Analysis of the Access Control using Krane

DAY 3

7 Kubernetes Admission Controllers

1. Fundamentals of Admission Controllers
2. Static Admission Controllers
    a. LimitRanger
    b. DefaultStorageClass
    c. AlwaysPullImages
3. Dynamic Admission Controllers
    a. Introduction to Custom Admission Controllers
    b. Working with Custom Admission WebHooks
    c. Authenticating API Servers
    d. Open Policy Agent (OPA) and Rego Policies
    e. Using OPA with Kubernetes
    f. OPA Gatekeeper
    g. OPA Kube-mgmt vs OPA Gatekeeper
4. Pod Security Context
5. Pod Security Policies
6. Pod Security Admission
    a. Pod Security Standards
    b. Policy Modes
    c. Applying Policies
7. Different Options to Write Custom Policies for K8s
8. **Hands-On Exercises**:
    a. Enforcing custom resource limits with LimitRanger
    b. Enforcing images are always pulled with Authorization
    c. Enforced trusted image using OPA Gatekeeper

Cloud-Native Security Expert

Detailed Syllabus

8 Kubernetes Data Security

1. Kubernetes Data Storage mechanisms
    a. Image Layers
    b. Container Mounts and Volumes
    c. Distributed Volumes in Kubernetes
    d. Persistent Volumes on Cloud
    e. Dynamically Provisioning Cloud Storage for Workloads
2. Managing secrets in traditional infrastructure
3. Managing secrets in containers at Scale
    a. Exploring Secret Storage Options
    b. Kubernetes Secrets Object
    c. Encrypted Configurations
    d. Managing Encryption Keys in External KMS
    e. Encrypting Secret Objects in Version Control Systems
    f. Mozilla SOPS for Secret OPerationS
    g. Introducing Secrets Store CSI Drivers
    h. Environment Variables and Volume Mounts
    i. Injecting Secrets with Hashicorp Vault
4. Sanning for Secrets Exposure
5. **Hands-on exercises**:
    a. Encrypting Secrets Data at rest
    b. Storing secrets securely using HashiCorp Vault
    c. Managing secrets using Sealed Secrets
    d. Automated Image scanning in
        i. Build stage
        ii. Release stage (artifact release)
        iii. Integration stage
        iv. Deployment stage

9 Kubernetes Network Security

1. Introduction to Kubernetes Networking
    a. Kubernetes Networking Architecture
    b. Challenges with Kubernetes Networking
2. Network Policies in Kubernetes
    a. Network Policy and Its Characteristics
    b. Anatomy of a Network Policy
3. Fallacies of Distributed Computing
4. Service Mesh Architecture
    a. Exploring Linkerd
    b. Zero Trust with Consul Connect
    c. Service Identities with Istio
5. **Hands-on exercises**:
    a. Implementing a Service Mesh with Istio
    b. Implementing a Service Mesh with Linkerd
    c. Enable mTLS in Service Mesh
    d. Writing custom Network Policies

Cloud-Native Security Expert

Detailed Syllabus

10 Defending Kubernetes Cluster

1. Compliance and Governance
    a. Kubernetes Compliance with Kubebench
    b. Kubernetes Compliance with Inspec
2. Threat Modeling for Kubernetes
3. Static Analysis of Kubernetes clusters
4. Building Secure Container Images
5. Dynamic and Runtime Security Analysis
6. Security Monitoring
7. **Hands-on exercises**:
    a. Kubernetes Least Privilege
    b. Kubernetes Static Analysis Analysis in CI/CD pipeline
    c. Defining Kubernetes Resource Quotas
    d. Kubernetes compliance using CIS benchmark
    e. Security monitoring of Kubernetes cluster using Wazuh
    f. Kubernetes Threat Detection using Falco
    g. Threat Hunting with Kubernetes audit logging

Cloud-Native Security Expert

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.

CCNSE exam is an online, task-oriented exam where you attempt to solve five challenges (tasks) in **12 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 CCNSE 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 CCNSE 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.

f @pdevsecops

@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