Study Plan

Kubernetes Security (K9-SEC)

BTECH TRAINING

boer technology

www.btech.id

About This Course

This course provides an overview of cloud security and container runtime security. It covers topics such as mitigating kernel vulnerabilities, deploying secure Kubernetes clusters, securing Kube API server, image security analysis, container security analysis, pod security policy, Kubernetes audit, Kubernetes network policy, Kubernetes workload considerations and Certified Kubernetes Security Exam Preparation. By the end of this course, you will have a solid understanding of how to secure your Kubernetes clusters and be prepared for the Certified Kubernetes Security Exam.

Summary

⏱ **Training Duration:** 32 Hours (4 Days)

Course Main Subjects

- Course Introduction
- Cloud Security Overview
- Container Runtime Overview
- Mitigating Kernel Vulnerabilities
- Deploy Secure Kubernetes Cluster
- Securing Kube API Server
- Image Security Analysis
- Container Security Analysis
- Pod Security Policy
- Kubernetes Audit
- Kubernetes Network Policy
- Kubernetes Workload Considerations
- Certified Kubernetes Security Exam Preparation

Target Audience

System Administrators, Cloud Administrators, Developers, Site Reliability Engineer.

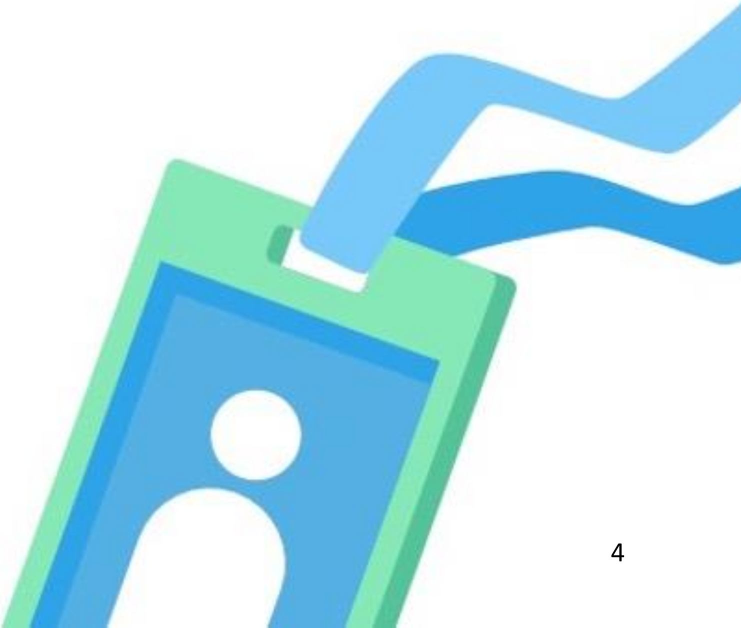
Prerequisites

- Kubernetes Administration (K9-ADM)

Learning Output

The learning topics will assist participants in :

1. Understanding Kubernetes security management
2. Creating container images at K8S Cluster for security
3. Managing Kubernetes security Cluster



Requirements

Have a laptop/computer with min. specifications and installed tools:

Operating System	Windows, Linux, or MacOs
Processor	Intel Core i3
Memory	4 GB RAM
SSH Client	Termius / Putty / MobaXTerm
Text Editor	Sublime Text / VSCode
Browser	Chrome and Firefox
VPN (Optional)	https://client.pritunl.com/

Facilities

- Virtual machine (available until H+5 post training)
- Class materials (Access 1 years)
- Certificate
- Recording (VITL)

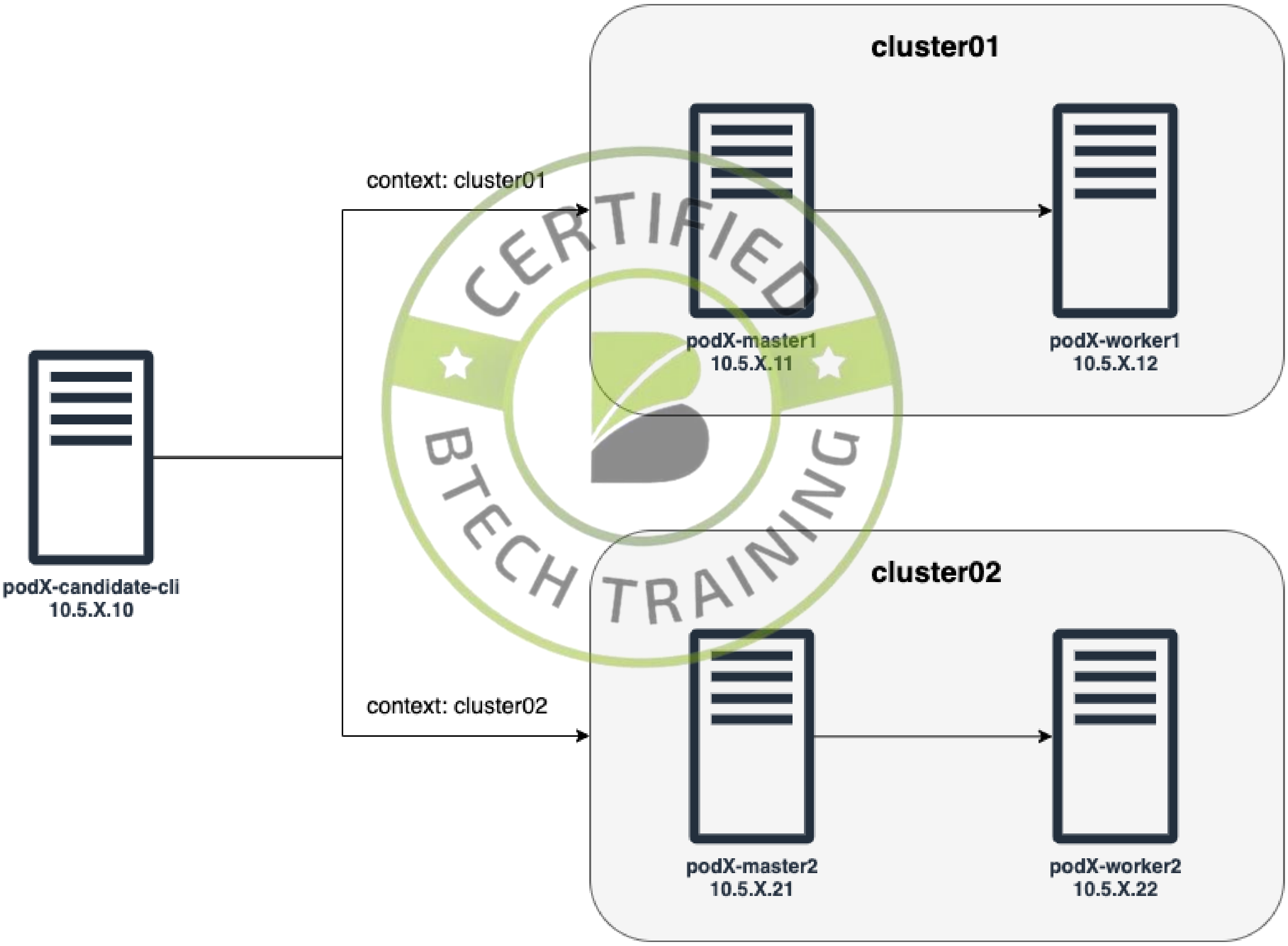
Certification

- Certificate of Course Completion
- Btech Internal Exam (optional)

Learning Strategies

- Theory
- Study Case
- Pre-Test & Post-Test
- Quiz / Internal Exam
- Hands-on Lab

Training Topology



Learning Modules

Training Plan	
Topic	**Outcome**
Security Overview	• Understand the basic principles of cloud security and the sources and types of attacks. • Learn about the 4Cs of security and how to apply the NIST Cybersecurity Framework and CIS Benchmarks. • Gain knowledge on how to use tools such as kube-bench to protect high-value assets. • Improve security team culture and limit access to sensitive information. • Practice setting up and deploying Kubernetes clusters and using candidate-cli. • Learn how to fix issues with API Server, Kubelet, and ETCD.

Secure Kubernetes Cluster	• Understand how to secure a Kubernetes cluster and where your container images come from. • Learn about different container runtimes and RuntimeClass, including gVisor and Kata. • Gain knowledge on how to use tools such as Gatekeeper to ensure trusted packages and protect the kernel. • Learn how to find kernel vulnerabilities and store sensitive data using Secret. • Practice implementing a container runtime sandbox with gVisor and using OPA Gatekeeper.
Secure the kube-apiserver	• Learn how to secure the kube-apiserver by enabling audit logs and configuring API auditing. • Understand the role of audit policies and how to implement Role-Based Access Control (RBAC) using Role and ClusterRole. • Gain knowledge on how to use RoleBinding and Pod Security Policies (PSP) to manage identity and access. • Learn how to manage persistent state from etcd and start using service accounts. • Practice creating and binding roles to limit access control with RBAC.

Networking	• Understand the basics of networking in Kubernetes and the role of services and firewalls. • Learn about key terms and expressions and the differences between stateful and stateless applications. • Gain knowledge on several network plugins and how to use chains and tables to manage rules with Netfilter and Firewalld. • Learn about Ingress Controllers and Service Meshes, including mTLS and network policies. • Practice implementing network security policies and working with load balancers, Ingress, and mTLS.
Workload Consideration	• Understand workload considerations and how to use tools such as Trivy and Falco to monitor for vulnerabilities and audit events. • Learn about SELinux and its enforcement modes, as well as Seccomp and AppArmor. • Gain knowledge on Dockerfile best practices to improve security. • Practice checking image vulnerabilities with Trivy and using Falco to monitor audit events. • Learn how to deny write access with an AppArmor profile.

Thank You

Another Course :

https://adinusa.id/pro-training