Study Plan

Kubernetes Security (K9-SEC)

BTECH TRAINING

boer technology

www.btech.id

About This Course

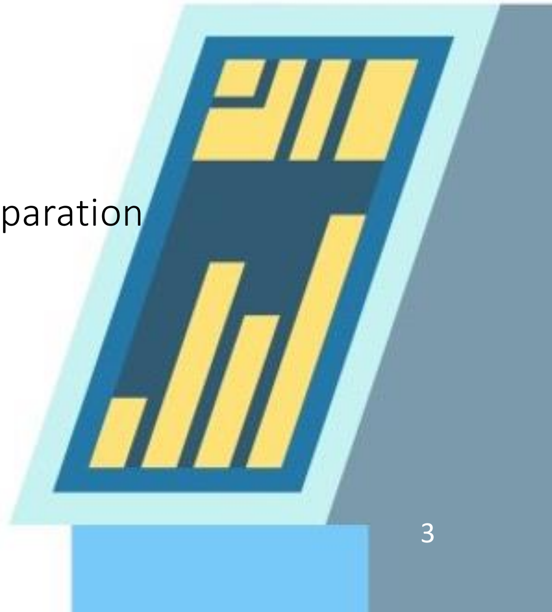
This course provides an overview of cloud security and container runtime security. It covers topics such as mitigating kernel vulnerabilities, deploying secure Kubernetes clusters, securing Kube API server, image security analysis, container security analysis, pod security policy, Kubernetes audit, Kubernetes 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. Version Kubernetes 1.29.15 on Ubuntu 22.04

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.

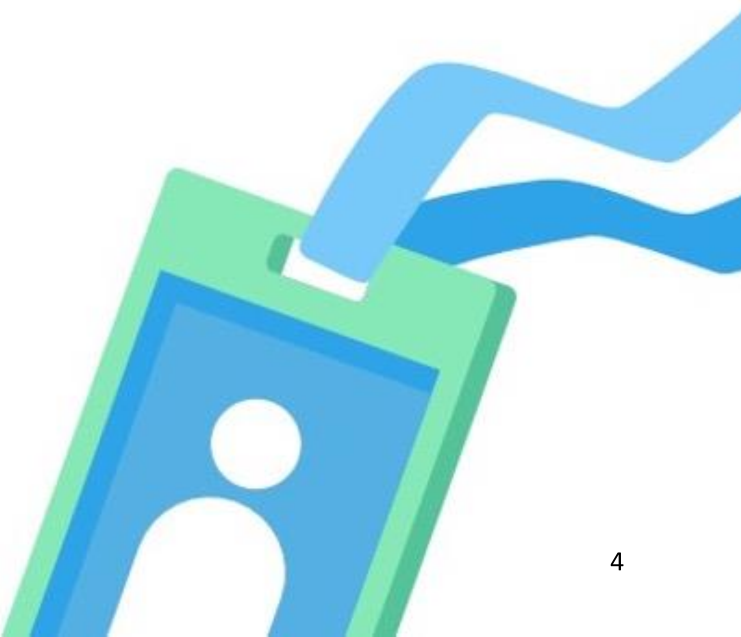
Prerequisites

- 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



Technical Requirements

Participants must have a laptop or computer with the following minimum specifications and tools installed:

Specification	Details
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 and Resources

Participants will have access to the following resources on and after the training:

- **Virtual machine lab** : Available until H+5 post-training for hands-on practice and experimentation.
- **Discussion group** : Available until H+30 post-training for ongoing support and collaboration with peers.
- **Class materials** : Access to all class materials for 1 year (start day one training)
- **Certificate** : Participants will receive a certificate of completion upon finishing the course.
- **Recording Class** : Access to recorded sessions for review and reinforcement of learning.

Terms and Conditions

Course Purchase Rules

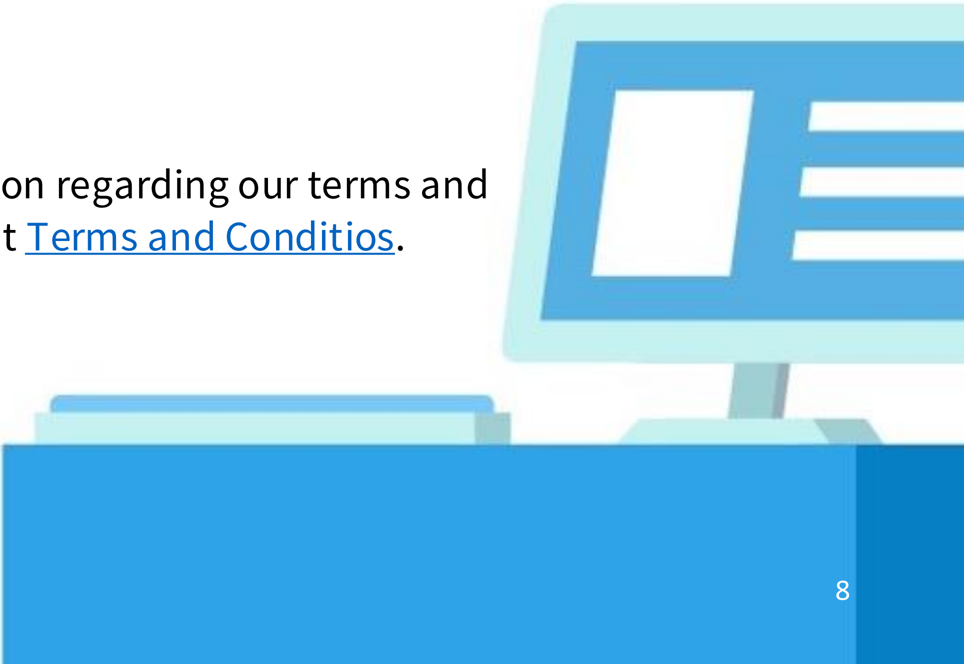
- **Registration**:
  Participants must register through the official ADINUSA website and fill out the registration form with accurate and complete information.
- **Payment**:
  Course payment must be made in full before access to training materials is granted. Accepted payment methods include bank transfer, credit card, and digital payment.
- **Purchase Confirmation**:
  After payment is received, participants will receive a confirmation email containing course details and instructions for accessing the materials.
- **Schedule Changes**:
  ADINUSA reserves the right to change the course schedule or replace instructors if necessary. Participants will be notified of such changes via email or whatsapp.

Terms and Conditions

Access Management

- **Access License**:
  Each participant will be granted an access license for 1 year, starting from the date of registration. This license includes access to all relevant training materials.
- **Use of Materials**:
  Training materials may only be used for personal purposes and may not be distributed, sold, or published without written permission from ADINUSA.
- **Account Security**:
  Participants are responsible for maintaining the confidentiality of their account information. ADINUSA is not liable for any losses arising from unauthorized account use.
- **Access Termination**:
  ADINUSA reserves the right to terminate a participant's access to training materials if violations of the applicable terms and conditions are found, including but not limited to unauthorized distribution of materials.

For detailed information regarding our terms and conditions, please visit Terms and Conditios.



Certification

Upon successful completion of the course, participants will receive two certificates with validation 2 years:

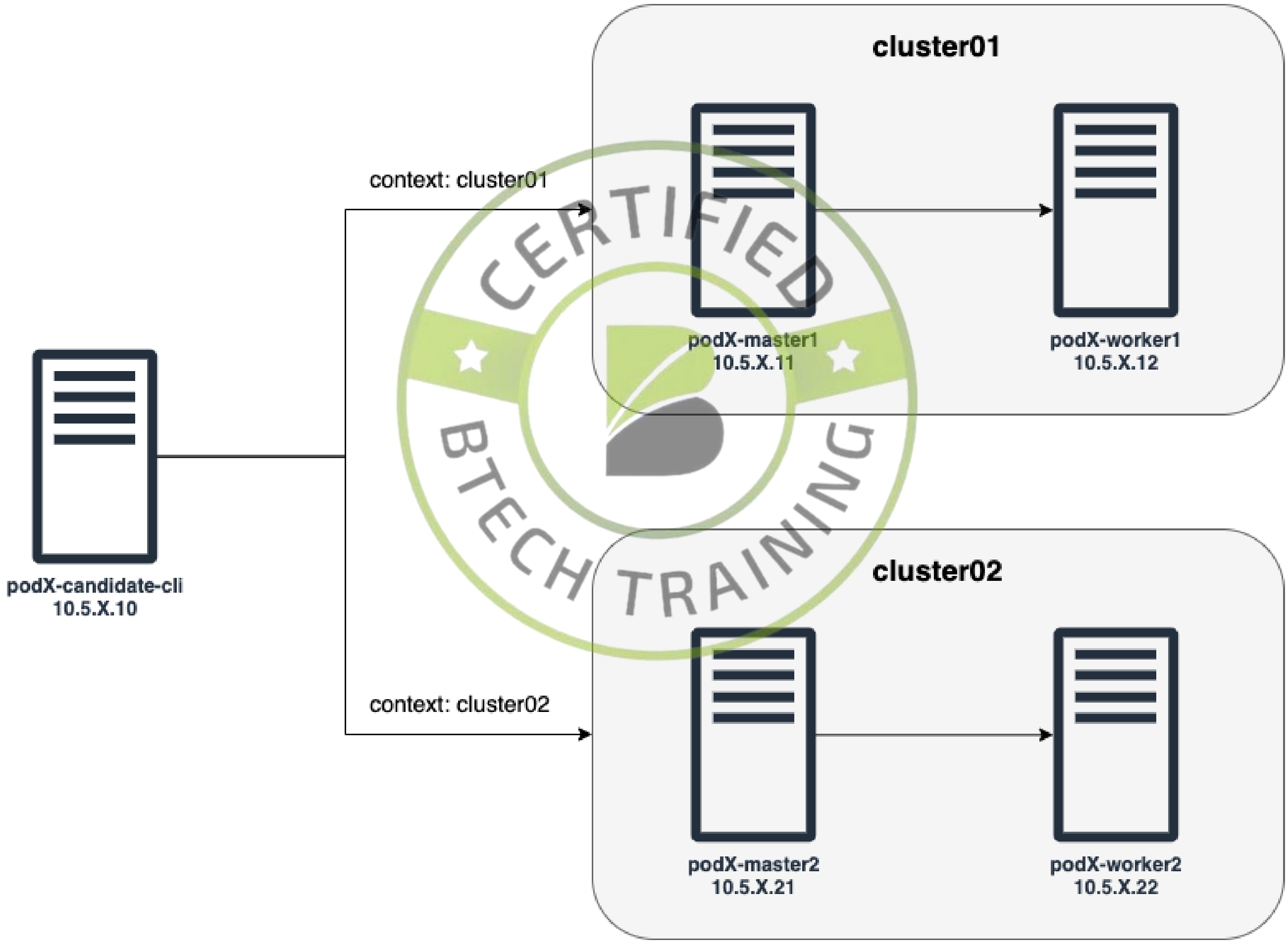
Physical Certificate

Digital Certificate

Learning Strategies

- Pre-Test
- Theory
- Hands-on Lab
- Post-Test
- Internal Exam
- Reporting
- Forum Discussion

Training Topology



Learning Modules

Training Plan	
Topic	**Outcome**
Security Overview	• Understand core concepts and threat sources in Kubernetes security. • Learn about NIST standards, CIS Benchmarks, and auditing with kube-bench. • Strengthen technical skills through hands-on labs and security evaluations.
Secure Kubernetes Cluster	• Learn how to secure containers with trusted images and runtime isolation tools like gVisor and Kata. • Understand the role of OPA Gatekeeper and best practices for protecting the kernel and sensitive data. • Reinforce knowledge through hands-on labs and quizzes on runtime sandboxing and Kubernetes secrets.

Secure the kube-apiserver	• Explore auditing and logging mechanisms to monitor API server activity effectively. • Master RBAC, Service Accounts, and Pod Security Policies for fine-grained access control. • Apply security practices through hands-on labs and quizzes on auditing, RBAC, and service accounts.
Networking	• Understand Kubernetes networking fundamentals including services, firewalls, and policy rules. • Explore secure traffic management using Ingress, mTLS, and Network Policies. • Practice real-world scenarios through labs on MetalLB, Linkerd, and network access control.
Workload Consideration	• Gain expertise in leveraging tools like Trivy and Falco to identify vulnerabilities and monitor security events in your workloads. • Master security enforcement mechanisms such as SELinux, Seccomp, and AppArmor to safeguard your containerized applications. • Refine your container security practices by adhering to Dockerfile best practices and enhancing manifest integrity through targeted labs and assessments.

Thank You

Explore our full course offerings in the training catalog:

https://adinusa.id/pro-training/catalogue

For further assistance, please contact us at:
Phone: +62 8111123242
Email: kontak@adinusa.id