Study Plan

DEVSECOPS (Development, Security & Operationals)

ADINUSA PRO TRAINING

About This Course

This course comprehensively covers key tools in the DevSecOps ecosystem. Participants will be guided in understanding the concepts and practical implementation of GitLab CI/CD for development and delivery automation. Additionally, they will learn about Kubernetes as a container orchestration platform, ArgoCD for efficient application management, and performance monitoring tools like Grafana and Prometheus for data analysis and visualization. The course also includes code analysis with SonarQube to identify and fix code issues and implement better coding practices. Participants will gain practical skills in implementing and managing these DevOps tools in a production context.

Summary

Training Duration: 32 Hours (4 Days)

Course Main Subjects

- Introduction to DevOps & DevSecOps
- Secure Software Development Life Cycle (SSDLC)
- DevSecOps Code
- Management and Variables CI/CD
- DevSecOps Pipeline
- DevSecOps Deployment and Testing
- System Monitoring and Logging
- Integration Bot ChatOps Teams

Target Audience

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

Prerequisites

- Kubernetes Administration (K9-ADM)
- Gitlab CI/CD (GL-CICD)

Learning Output

The learning topics will assist participants in :

- Basic to complex understanding for DevSecOps implementation in scope of work.
- Participants can perform analyses using unit testing and security testing methods to ensure each process runs according to standards
- Participants can perform daily operations for each activity in CI/CD

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

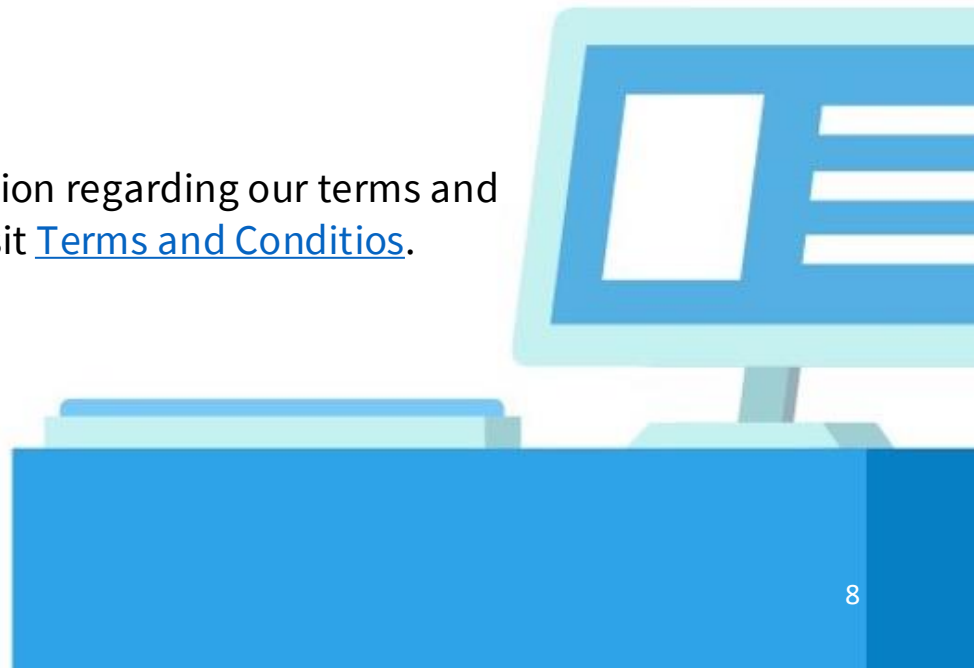
- **Registration**:
  Participants must register through the official ADINUSA website and fill out the registration form with accurate and complete information.
- **Payment**:
  Course payment must be made in full before access to training materials is granted. Accepted payment methods include bank transfer, 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:

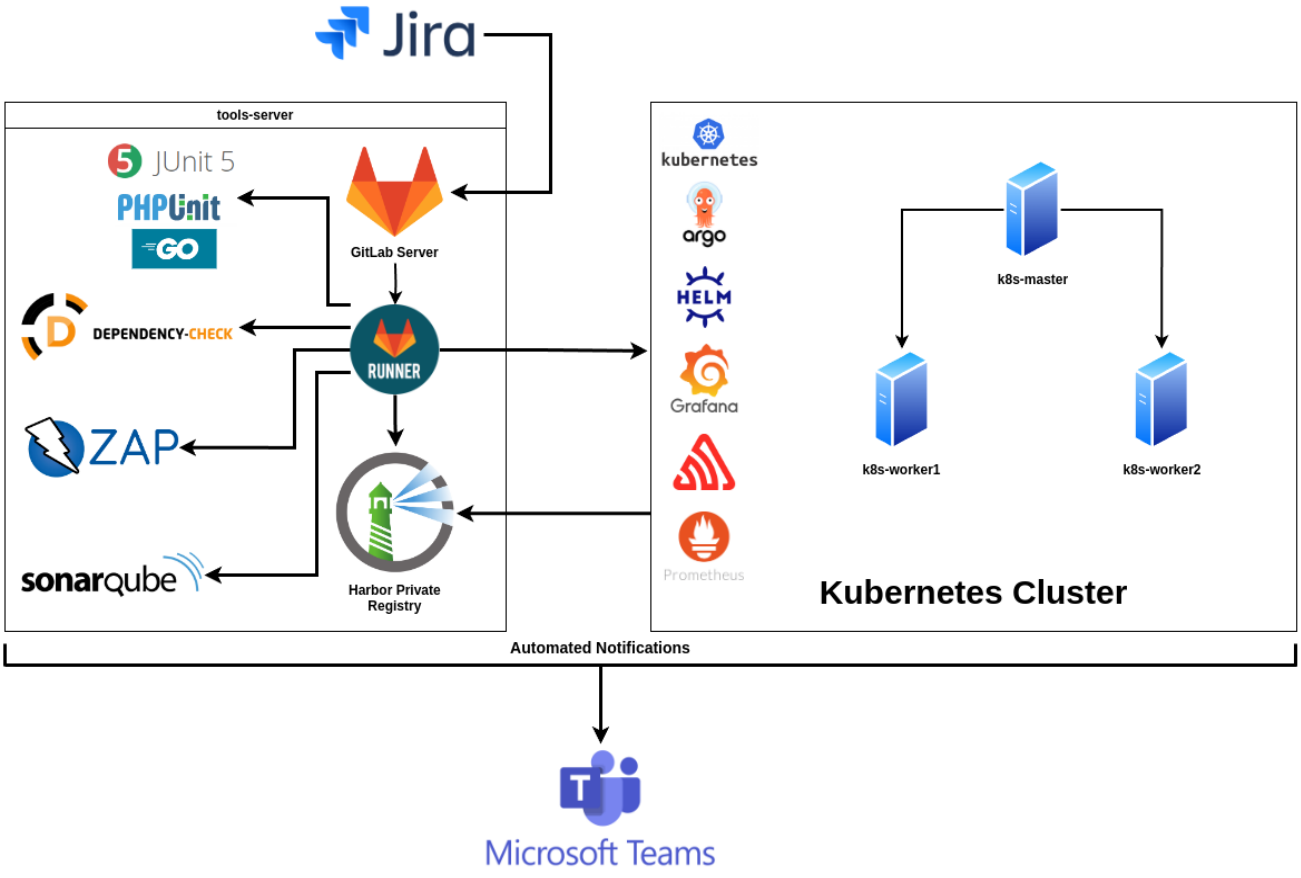
Physical Certificate

Digital Certificate

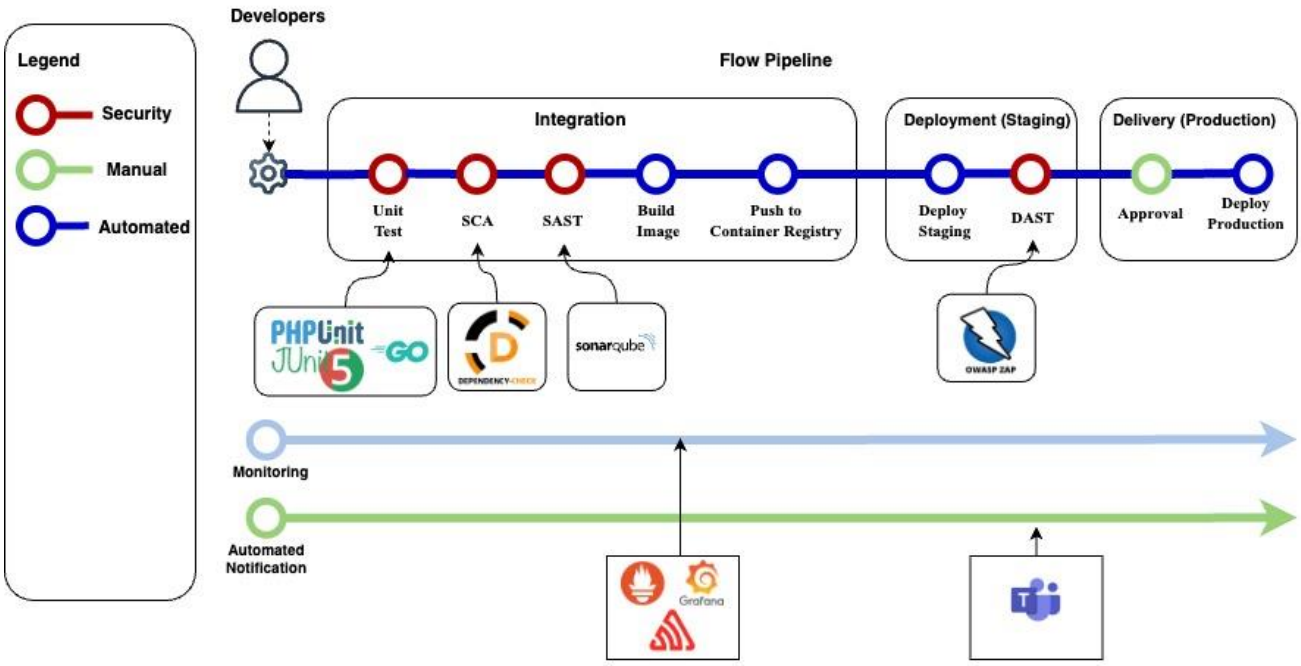
Learning Strategies

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

Topology Training



Topology Training : Pipeline Flow



Learning Modules

Training Plan	
Topic	**Outcome**
Introduction to DevOps & Devsecops	• Participants will understand how DevOps enhances efficiency, collaboration, and business outcomes. • Participants will learn to integrate speed, collaboration, and security throughout the development lifecycle. • Participants will recognize the benefits and challenges of DevSecOps and strategies to address them. • Participants will assess and improve their organization's DevSecOps maturity level.
Secure Software Development Life Cycle (SSDLC)	• Participants will grasp the fundamentals of the Secure Software Development Lifecycle (SSDLC) and its importance in integrating security throughout development. • Participants will learn how to implement and manage SSDLC processes effectively within their development environment.

DevSecOps Code	• Participants will learn practices for writing secure code to prevent vulnerabilities. • Participants will understand how to ensure code quality and manage libraries using Software Composition Analysis (SCA). • Participants will recognize and address known vulnerabilities through CVE references. • Participants will identify and mitigate common coding weaknesses using CWE guidelines.Participants will implement tools and techniques for scanning code to find security issues. • Participants will develop effective branching strategies for managing code changes and collaboration.
CI/CD	• Participants will learn to plan and manage projects using Jira. • Participants will understand how to integrate ticketing systems with Jira for streamlined issue tracking. • Participants will grasp the core concepts of GitLab Continuous Integration (CI). • Participants will be able to create and integrate CI/CD pipelines within GitLab. • Participants will learn to incorporate security measures throughout each stage of the CI/CD pipeline.

DevSecOps Pipeline	• Participants will understand the basics of static security testing and its role in finding vulnerabilities early. • Participants will learn to integrate SonarQube for static analysis in repositories and CI/CD pipelines. • Participants will be able to detect and remediate security issues in their source code. • Participants will manage app builds, create container images, and perform security scans on containers. • Participants will develop unit tests and integrate them into CI/CD pipelines for automated testing.
DevSecOps Deployment	• Participants will learn to configure environment variables across different environments. • Participants will understand how to deploy applications using Kubernetes. • Participants will manage deployments in both staging and production environments.
DevSecOps Testing	• Participants will understand the principles of dynamic security testing. • Participants will learn to integrate Dynamic Application Security Testing (DAST) into CI/CD pipelines. • Participants will gain skills in interpreting and addressing DAST findings.

Monitoring & Logging	• Participants will monitor CI/CD processes, infrastructure, and application performance. • Participants will track and manage application errors using Sentry. • Participants will enforce security policies through code and policy-based controls. • Participants will learn to generate and analyze deployment audit logs.
ChatOps	• Participants will integrate ChatOps tools with Microsoft Teams for enhanced collaboration.

Thank You

Another Course :

https://adinusa.id/pro-training