COURSE TABLE OF CONTENTS

# Trivy Security Scanning Fundamentals

OEM: Open Source • Duration: 2 Days (16 hrs)

## COURSE MODULES & TOPICS

### Module 1: Security Scanning Fundamentals
- DevSecOps fundamentals
- Vulnerability management concepts
- CVE and CVSS overview
- OWASP security basics

### Module 2: Introduction to Trivy
- Trivy architecture and features
- Supported scanning capabilities
- Common use cases

### Module 3: Trivy Installation and Configuration
- Linux installation steps
- Docker-based installation
- CLI configuration
- Database updates

### Module 4: Container Image Scanning
- Scanning Docker images
- Detecting OS package vulnerabilities
- Identifying application dependency issues

### Module 5: Vulnerability Analysis and Remediation
- CVE identification
- Severity levels and prioritization
- Remediation strategies

### Module 6: Filesystem and Repository Scanning
- Scanning source code directories
- Analyzing package dependencies
- Scanning Git repositories
- Security assessment of repositories

### Module 7: Reporting and Output Formats
- Generating table, JSON, SARIF reports
- Filtering by severity
- Customizing report outputs

### Module 8: Dependency and Filesystem Security
- Software composition analysis (SCA)
- Detecting package vulnerabilities

© Koenig Solutions

### Module 9: Secret Scanning
- Detecting exposed API keys
- Identifying passwords, tokens, credentials

### Module 10: Infrastructure as Code (IaC) Security Scanning
- Scanning Terraform files
- Kubernetes YAML analysis
- Dockerfile and Helm chart scanning

### Module 11: Kubernetes Security Scanning
- Cluster scanning
- Workload configuration checks
- Detecting Kubernetes misconfigurations

### Module 12: SBOM Generation
- Software Bill of Materials (SBOM)
- SPDX and CycloneDX formats

### Module 13: CI/CD Pipeline Integration
- Integrating with Jenkins
- GitHub Actions setup
- GitLab CI/CD and Azure DevOps integration

### Module 14: Security Gates and Policies
- Setting severity thresholds
- Configuring exit codes
- Pipeline failure policies

### Module 15: Compliance and Remediation Reporting
- Generating misconfiguration reports
- Vulnerability tracking
- Remediation workflows

### Module 16: Trivy CLI Commands Reference
- Version checks
- Image, filesystem, repo, IaC, Kubernetes scans
- Report generation and filtering
- Enforcing exit codes

### Module 17: End-to-End DevSecOps Project
- Implementing Trivy in CI/CD pipelines
- Automated image and IaC scanning
- Secret detection and SBOM generation
- Security gates and remediation