COURSE TABLE OF CONTENTS

Aqua Security (AquaSec) Administration

OEM: Koenig Original • Duration: 5 Days (40 hrs)

COURSE MODULES & TOPICS

Module 1: Container Security Fundamentals
- Container security basics and challenges
- DevSecOps concepts
- Cloud-native security overview

Module 2: Aqua Security Platform Overview
- Aqua Platform and key capabilities
- Aqua Cloud Native Security Platform
- Core components and integrations

Module 3: Aqua Security Architecture
- Aqua Console, Gateway, Scanner, Enforcer
- Database and integration architecture

Module 4: Installation and Initial Configuration
- Deployment prerequisites and sizing
- Installation options
- Initial configuration steps

Module 5: User and Role Administration
- User management
- Role-based access control (RBAC)
- Authentication configuration

Module 6: Platform Management
- Console navigation
- System settings
- Certificates and licensing

Module 7: Container Image Security
- Image security fundamentals
- Registry integration (Docker Hub, ECR, ACR, GCR)
- Vulnerability scanning and assessment

Module 8: Image Assurance and Compliance
- Image trust and assurance policies
- Malware scanning
- CIS benchmarks and vulnerability compliance

Module 9: Vulnerability Reporting and Remediation
- Vulnerability reports
- Risk assessment
- Remediation of vulnerable images

© Koenig Solutions

Module 10: Kubernetes Security Integration
- Kubernetes security fundamentals
- Integrating Aqua with Kubernetes and OpenShift

Module 11: Enforcer Deployment and Runtime Protection
- Deploying Aqua Enforcers with Helm
- Container runtime monitoring and protection

Module 12: Admission Control and Network Security
- Kubernetes admission policies
- Deployment enforcement
- Container segmentation and network policy concepts

Module 13: Threat Detection and Response
- Suspicious process detection
- Anomalous activity monitoring
- Blocking unauthorized container execution

Module 14: DevSecOps and Secure SDLC
- Shift-left security principles
- Secure software development lifecycle

Module 15: CI/CD Pipeline Integration
- Integrating Aqua with Jenkins, GitLab CI/CD, GitHub Actions, Azure DevOps
- Container image scanning during builds

Module 16: Pipeline Security and Policy Enforcement
- Security gates and vulnerability thresholds
- Preventing deployment of vulnerable images

Module 17: Infrastructure as Code and Supply Chain Security
- IaC security concepts and Terraform integration
- Image integrity, SBOM, provenance and trust

Module 18: Automation and API Integration
- Aqua APIs and CLI usage
- Automated security workflows

Module 19: Advanced Policy Management
- Custom security policies
- Policy management best practices

Module 20: Compliance and Audit Management
- CIS Kubernetes and Docker benchmarks
- Regulatory controls
- Audit logs and security event reporting

Module 21: Monitoring, Troubleshooting and Maintenance
- Runtime events and dashboards
- Alerting and monitoring
- Troubleshooting Scanner, Enforcer, Gateway

- Backup, upgrades, and maintenance

Module 22: Enterprise Deployment Best Practices

- Operational practices
- Enterprise Aqua Security deployment architecture

Module 23: End-to-End DevSecOps Project

- Secure container image build and deployment
- Vulnerability scanning and remediation
- Kubernetes workload protection
- CI/CD security gate implementation
- Runtime security monitoring and reporting