Container Image Scanning and Registry Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid adoption of Cloud-Native architectures and DevSecOps practices has made containerization the backbone of modern software deployment. However, this agility introduces critical new attack surfaces, primarily within the container Software Supply Chain specifically the image build and registry storage phases. Container Image Scanning and Registry Security Training Course provides a deep-dive into securing the foundational components of your containerized environment. Participants will master proactive, Shift-Left Security techniques, learning how to implement automated Vulnerability Management and robust Policy as Code to detect, prioritize, and remediate risks within container images before they ever reach production.

This hands-on program moves beyond theoretical concepts, focusing on practical implementation of Security Scanning and Registry Hardening across modern platforms like Kubernetes and major cloud providers. You?ÇÖll gain proficiency in leveraging cutting-edge open-source and commercial tools to enforce Zero Trust principles, manage Image Integrity through signing and verification, and establish continuous Compliance throughout the container lifecycle. Secure your entire Software Development Lifecycle (SDLC), transform your security posture, and minimize your exposure to critical threats like supply chain attacks and misconfigurations by becoming an expert in container image and registry defense.

Programme Curriculum

Container Image Scanning and Registry Security Training Course

Introduction

The rapid adoption of Cloud-Native architectures and DevSecOps practices has made containerization the backbone of modern software deployment. However, this agility introduces critical new attack surfaces, primarily within the container Software Supply Chain specifically the image build and registry storage phases.

Container Image Scanning and Registry Security Training Course provides a deep-dive into securing the foundational components of your containerized environment. Participants will master proactive, Shift-Left Security techniques, learning how to implement automated Vulnerability Management and robust Policy as Code to detect, prioritize, and remediate risks within container images before they ever reach production.

This hands-on program moves beyond theoretical concepts, focusing on practical implementation of Security Scanning and Registry Hardening across modern platforms like Kubernetes and major cloud providers. You? ÇÖll gain proficiency in leveraging cutting-edge open-source and commercial tools to enforce Zero Trust principles, manage Image Integrity through signing and verification, and establish continuous Compliance throughout the container lifecycle. Secure your entire Software Development Lifecycle (SDLC), transform your security posture, and minimize your exposure to critical threats like supply chain attacks and misconfigurations by becoming an expert in container image and registry defense.

Course Duration

5 days

Course Objectives

1. Shift-Left Container Security into the CI/CD Pipeline.
2. Implement automated Vulnerability Scanning and CVE triage for images.
3. Design and enforce Policy-as-Code for container image acceptance.
4. Master Container Registry Hardening best practices and access controls.
5. Leverage Image Signing and Notary to ensure Image Integrity.
6. Understand and mitigate Supply Chain Attacks in container environments.
7. Analyze and remediate common container Misconfigurations and embedded Secrets.
8. Integrate scanning tools with Kubernetes Admission Controllers for runtime defense.
9. Develop strategies for managing vulnerabilities in Base Images and dependencies.
10. Ensure Regulatory Compliance using automated scanning.
11. Implement Continuous Scanning for newly disclosed Zero-Day vulnerabilities.
12. Utilize SBOMs for transparency and risk assessment.
13. Configure Role-Based Access Control for registry security.

Target Audience

1. DevSecOps Engineers
2. Cloud Security Architects
3. Software Engineers/Developers
4. Security Operations (SecOps) Analysts
5. Vulnerability Management Specialists
6. Kubernetes Administrators and SREs
7. Cloud Engineers (AWS, Azure, GCP)
8. IT Auditors and Compliance Professionals

Course Modules

Module 1: Foundations of Container Image & Registry Security

- Understanding the container Attack Surface and key risks.
- Container Security and Traditional Security Paradigms.
- Deep dive into Docker/OCI Image structure and layers.

- The role of Container Registries in the Software Supply Chain.
- Introduction to Shift-Left Security principles.
- Case Study: Analyzing the Capital One Breach to highlight how misconfigurations and excessive permissions in cloud and container resources lead to data exposure.

Module 2: Static Container Image Scanning for Vulnerabilities

- Comparing Trivy, Clair, and Anchore Engine.
- Vulnerability Triage and prioritizing remediation by severity and exploitability.
- Finding vulnerabilities in the Base Image and application dependencies.
- Generating and utilizing the Software Bill of Materials for transparency.
- Handling false positives and establishing a security quality gate.
- Case Study: The Docker Hub Breach of 2019, focusing on how compromised user credentials and the lack of robust registry security led to potential image tampering exposure.

Module 3: Automating Security in the CI/CD Pipeline

- Integrating scanning into GitLab, GitHub Actions, and Jenkins pipelines.
- Failing builds based on Policy as Code thresholds
- Scanning for embedded Secrets, Hardcoded Credentials, and excessive metadata.
- Best practices for creating minimal, secure Base Images
- Implementing Pre-Commit Hooks for early developer feedback.
- Case Study: Examining a fictional CI/CD Pipeline Hijack, where a threat actor injects malicious code into a build agent, demonstrating the need for image signing and build environment hardening.

Module 4: Container Registry Hardening and Access Control

- Configuring strong Role-Based Access Control in registries
- Network segmentation and using Private Registries exclusively.
- Image Retention Policies and removal of stale, vulnerable images.
- Securing the registry API and enforcing TLS/HTTPS only.
- Implementing Registry Mirroring and geo-replication securely.
- Case Study: The NotPetya Attack, highlighting the danger of compromised software distribution points and the critical need for registry integrity and strong access policies.

Module 5: Ensuring Image Integrity with Notary and Signing

- Understanding Image Trust and the problem of image tampering.
- Implementation of Docker Content Trust and other signing mechanisms.
- Using Notary and TUF for key management.
- Verifying image signatures before deployment to the runtime.
- Key Management best practices for code and image signing certificates.
- Case Study: Simulating a Malicious Image Injection scenario, where an unauthorized image is pushed to a registry, illustrating how image signing and verification prevent deployment.

Module 6: Runtime Policy Enforcement with Kubernetes

- Introduction to Kubernetes Admission Controllers
- Enforcing deployment policies using Kyverno or OPA/Gatekeeper.
- Blocking images with unpatched critical vulnerabilities or insecure configurations.
- Preventing deployments that attempt to run containers as the Root User.

- Implementing mandatory resource limits and Security Contexts.
- Case Study: The Tesla Kubernetes Cluster Breach, where attackers gained access through an unprotected console, demonstrating the failure of RBAC and the need for rigorous runtime admission controls.

Module 7: Advanced Vulnerability and Risk Management

- Continuous Scanning of dormant images for newly disclosed CVEs
- Prioritizing remediation based on Contextual Risk and environmental factors.
- Strategies for dealing with vulnerabilities in third-party and vendor images.
- Automated patching and Golden Image management workflows.
- Integrating scan results with Security Information and Event Management systems.
- Case Study: The Log4Shell Vulnerability, showing the widespread impact and the critical role of continuous registry scanning and SBOMs for rapid identification and patching.

Module 8: Compliance and Future Trends in Container Security

- Mapping scanning results to Compliance Frameworks
- Cloud Security Posture Management for container environments.
- Introduction to Confidential Containers and advanced isolation techniques.
- Leveraging eBPF for deeper runtime security and monitoring.
- Developing an Incident Response plan specific to container breaches.
- Case Study: A Compliance Audit Failure scenario, where a company is penalized for deploying non-compliant images, underscoring the necessity of automated compliance checks.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org **or call** +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com