+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/09/2026

Sign up

Chainguard Training: Securing the Software Supply Chain

2 days (14 hours)

Overview

Chainguard is a solution specialized in securing the software supply chain. It offers minimal, hardened container images designed to reduce vulnerabilities, improve the traceability of software components, and strengthen the security of cloud-native deployments.

Our Chainguard training will help you master best practices in Supply Chain Security as applied to containers, CI/CD pipelines, and Kubernetes environments.

You will learn how to use Chainguard Containers, compare standard images with hardened images, and leverage SBOMs, signatures, attestations, and software provenance to ensure the reliability of your deployments.

By the end of the training, you will be able to integrate Chainguard into your DevSecOps workflows, verify your images with Cosign, reduce the attack surface of your containers, and implement security controls in your Kubernetes pipelines and clusters.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the challenges of supply chain security as they apply to containers
- Use Chainguard images to reduce vulnerabilities and the attack surface
- Leverage SBOMs, signatures, attestations, and proofs of origin
- Verify images with Cosign and integrate these checks into a CI/CD pipeline

- Secure Kubernetes deployments with trusted images
- Developing a container image governance strategy for your organization

Target Audience

- DevOps and DevSecOps engineers
- SRE and Platform Engineers
- Cloud-native security engineers
- Kubernetes administrators
- Cloud architects and CI/CD managers

Prerequisites

- Basic knowledge of containers and Docker
- Basic understanding of CI/CD or application deployment
- General knowledge of Kubernetes recommended

Technical prerequisites

- A computer running Linux, macOS, or Windows with WSL2
- Ensure a stable internet connection

Chainguard Training Program

[Day 1 - Morning]

Understanding Chainguard and the challenges of supply chain security

- Understand Chainguard’s role in a modern DevSecOps strategy
- Identifying risks related to container images: CVEs, obsolete dependencies, oversized images, and lack of traceability
- Understanding the principles of Supply Chain Security: provenance, signatures, attestations, SBOM
  and compliance
- Position Chainguard against traditional approaches to scanning, patching, and image hardening
- Discover the Chainguard ecosystem: Chainguard Containers, Wolfi, apko, melange, Sigstore, and Cosign
- Hands-on workshop: analyze a standard image, identify its vulnerabilities, and compare the approach with a Chainguard image

[Day 1 - Afternoon]

Hardened images, SBOM, and attack surface reduction

- Understanding the philosophy of minimalist and distroless images
- Using Chainguard Containers to replace traditional application images
- Reducing the attack surface by removing shells, package managers, and unnecessary dependencies
- Understanding the role of SBOMs in inventorying embedded software components
- Reading and leveraging metadata associated with a container image
- Hands-on workshop: Replacing a base image with a Chainguard image and comparing size, dependencies, and vulnerabilities

Signatures, attestations, and verification with Cosign

- Understand image signatures, attestations, and proofs of origin
- Using Sigstore and Cosign to verify the authenticity of an image
- Retrieve and verify the SBOMs associated with a Chainguard image
- Understanding SLSA compliance levels and their relevance for audits
- Implementing a reproducible verification process within a team workflow
- Hands-on workshop: Verifying the signature, provenance, and SBOM of a Chainguard image with Cosign

[Day 2 - Morning]

CI/CD integration and container security policy

- Integrating Chainguard into an existing CI/CD pipeline
- Automate the verification of images, signatures, SBOMs, and attestations
- Implement blocking rules for non-compliant images
- Define a policy for using base images within the organization
- Reduce scanner noise and prioritize truly exploitable vulnerabilities
- Hands-on workshop: Adding an image verification step to a CI/CD pipeline

[Day 2 - Afternoon]

Kubernetes, admission control, and secure deployment

- Understand the risks associated with deploying uncontrolled images in Kubernetes
- Define admission rules to control authorized images
- Validate signatures and metadata before deployment
- Organize a trusted image strategy by environment
- Aligning Chainguard with GitOps, Platform Engineering, and DevSecOps practices
- Hands-on workshop: Defining a Kubernetes deployment policy based on verified images

Governance, Migration, and End-to-End Scenario

- Developing a migration strategy from traditional images to Chainguard images
- Define responsibilities among DevOps, security, development, and platform teams

- Implementing image governance: internal catalog, exceptions, validation, and monitoring
- Prepare audit-ready elements: SBOM, provenance, signatures, and control policy
- Identify the limitations, costs, prerequisites, and success criteria for a Chainguard deployment
- Hands-on workshop: Design a roadmap for securing the containerized supply chain for an enterprise application

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.