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

Mis à jour le 09/06/2026

S'inscrire

Formation Chainguard : sécuriser la supply chain logicielle

2 jours (14 heures)

Présentation

Chainguard est une solution spécialisée dans la sécurisation de la supply chain logicielle. Elle propose des images conteneurs minimales, durcies et conçues pour réduire les vulnérabilités, améliorer la traçabilité des composants logiciels et renforcer la sécurité des déploiements cloud native.

Notre formation Chainguard vous permettra de maîtriser les bonnes pratiques de Supply Chain Security appliquées aux conteneurs, aux pipelines CI/CD et aux environnements Kubernetes.

Vous apprendrez à utiliser les Chainguard Containers, à comparer des images classiques avec des images durcies, à exploiter les SBOM, les signatures, les attestations et la provenance logicielle pour fiabiliser vos déploiements.

À l'issue de la formation, vous serez en mesure d'intégrer Chainguard dans vos workflows DevSecOps, de vérifier vos images avec Cosign, de réduire la surface d'attaque de vos conteneurs et de mettre en place des contrôles de sécurité dans vos pipelines et clusters Kubernetes.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les enjeux de supply chain security appliqués aux conteneurs
- Utiliser les images Chainguard pour réduire les vulnérabilités et la surface d'attaque
- Exploiter les SBOM, signatures, attestations et preuves de provenance
- Vérifier les images avec Cosign et intégrer ces contrôles dans une pipeline CI/CD

- Sécuriser les déploiements Kubernetes avec des images de confiance
- Construire une stratégie de gouvernance des images conteneurs en entreprise

Public visé

- Ingénieurs DevOps et DevSecOps
- Ingénieurs SRE et Platform Engineers
- Ingénieurs sécurité cloud native
- Administrateurs Kubernetes
- Architectes cloud et responsables CI/CD

Pré-requis

- Connaissances de base en conteneurs et Docker
- Notions de CI/CD ou de déploiement applicatif
- Connaissances générales de Kubernetes recommandées

Pré-requis techniques

- Disposer d’un ordinateur avec Linux, macOS ou Windows avec WSL2
- Prévoir une connexion Internet stable

Programme de notre formation Chainguard

[Jour 1 - Matin]

Comprendre Chainguard et les enjeux de supply chain security

- Comprendre le rôle de Chainguard dans une stratégie DevSecOps moderne
- Identifier les risques liés aux images conteneurs : CVE, dépendances obsolètes, images trop larges et absence de traçabilité
- Comprendre les principes de Supply Chain Security : provenance, signatures, attestations, SBOM et conformité
- Positionner Chainguard face aux approches classiques de scan, patching et durcissement d’images
- Découvrir l’écosystème Chainguard : Chainguard Containers, Wolfi, apko, melange, Sigstore et Cosign
- Atelier pratique : analyser une image standard, identifier ses vulnérabilités et comparer l’approche avec une image Chainguard

[Jour 1 - Après-midi]

Images durcies, SBOM et réduction de surface d’attaque

- Comprendre la philosophie des images minimalistes et distroless
- Utiliser les Chainguard Containers pour remplacer des images applicatives classiques
- Réduire la surface d'attaque en supprimant shells, gestionnaires de paquets et dépendances inutiles
- Comprendre le rôle des SBOM pour inventorier les composants logiciels embarqués
- Lire et exploiter les métadonnées associées à une image conteneur
- Atelier pratique : remplacer une image de base par une image Chainguard et comparer taille, dépendances et vulnérabilités

Signatures, attestations et vérification avec Cosign

- Comprendre les signatures d'images, attestations et preuves de provenance
- Utiliser Sigstore et Cosign pour vérifier l'authenticité d'une image
- Récupérer et vérifier les SBOM associés à une image Chainguard
- Comprendre les niveaux de conformité SLSA et leur intérêt pour les audits
- Mettre en place une vérification reproductible dans un workflow d'équipe
- Atelier pratique : vérifier la signature, la provenance et le SBOM d'une image Chainguard avec Cosign

[Jour 2 - Matin]

Intégration CI/CD et politique de sécurité conteneurs

- Intégrer Chainguard dans une chaîne CI/CD existante
- Automatiser la vérification des images, signatures, SBOM et attestations
- Mettre en place des règles de blocage sur les images non conformes
- Définir une politique d'usage des images de base dans l'organisation
- Réduire le bruit des scanners et prioriser les vulnérabilités réellement exploitables
- Atelier pratique : ajouter une étape de vérification d'image dans une pipeline CI/CD

[Jour 2 - Après-midi]

Kubernetes, admission control et déploiement sécurisé

- Comprendre les risques liés au déploiement d'images non maîtrisées dans Kubernetes
- Définir des règles d'admission pour contrôler les images autorisées
- Valider les signatures et métadonnées avant déploiement
- Organiser une stratégie d'images de confiance par environnement
- Aligner Chainguard avec les pratiques GitOps, Platform Engineering et DevSecOps
- Atelier pratique : définir une politique de déploiement Kubernetes basée sur des images vérifiées

Gouvernance, migration et cas final

- Construire une stratégie de migration depuis des images classiques vers des images Chainguard
- Définir les responsabilités entre équipes DevOps, sécurité, développement et plateforme

- Mettre en place une gouvernance des images : catalogue interne, exceptions, validation et suivi
- Préparer les éléments attendus en audit : SBOM, provenance, signatures et politique de contrôle
- Identifier les limites, coûts, prérequis et critères de succès d'un déploiement Chainguard
- Atelier pratique : concevoir une trajectoire de sécurisation de la supply chain conteneurisée pour une application d'entreprise

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.