Kubernetes – Sécuriser son infrastructure

Prix : 1 750 €HT

Durée : 2 jours

Code de Référence : KUBSEC

Catalogue Cloud Native et DevOps

Objectifs de la formation

A l'issue de cette formation, vous serez capable de :

- Identifier les bonnes pratiques de sécurité dans Kubernetes
- Mettre en œuvre des outils de sécurisation des registres de conteneurs
- Appliquer des outils de conformité dans un environnement Kubernetes
- Déployer des outils de sécurité dynamiques dans un cluster Kubernetes
- Concevoir et intégrer des politiques de sécurité adaptées à vos besoins

Public

Cette formation s'adresse aux administrateurs systèmes, DevOps, DevSecOps, développeurs, architectes, SRE.

Prérequis

Bonnes connaissances de Linux / Unix, Docker, conteneurs, réseau SDN. Avoir suivi les formations KUBORCH et KUBAV ou avoir un niveau équivalent.

Programme de la formation

Jour 1 – Matin
Principes fondamentaux et socles technologiques de sécurité

Fondamentaux des conteneurs et de la sécurité

- Évolution vers les architectures basées sur les conteneurs
- Caractéristiques d'un conteneur (immuabilité, portabilité)
- Risques associés (surface d'attaque, isolation insuffisante)

Sécurité des technologies sous-jacentes

- Fonctionnement des namespaces (PID, NET, MNT, etc.)
- Control Groups (cgroups) : isolation des ressources
- Rôle du noyau et des OS adaptés aux conteneurs

Exemples de travaux pratiques (à titre indicatif) :
Déploiement d'un cluster EKS sur AWS
Création/configuration d'un utilisateur
Personnalisation de kubeconfig pour accès sécurisé

Jour 1 – Après-midi
Sécurisation des moteurs de containers et registres
Sécurité Docker et OCI

- Sécurisation du runtime CRI, de containerd et de ses sockets
- Bonnes pratiques Dockerfile (USER, COPY, RUN, etc.)
- Sécurité des images : scan automatique, vulnérabilités
- Qu'en dit l'ANSSI ?

Écosystème OCI et évolutions

- Containerd et runc : remplacement de Docker Engine
- Initiative OCI : standardisation des formats
- MicroVM et Unikernels : sécurité renforcée à l'exécution

Exemples de travaux pratiques (à titre indicatif) :
Déploiement du registre Harbor
Découverte des fonctionnalités de sécurité du registre
Filtrage par worker Kubernetes
Sécurisation des accès au registre (authentification, rôles)
Utilisation de Trivy pour scan d'image et détection de CVE

Jour 2 – Matin
Sécurité réseau, RBAC et Service Mesh
Sécurité dans l'orchestration Kubernetes

- Menaces spécifiques au CaaS (exposition API, etc.)
- Durcissement du cluster et des Pods : SecurityContext, seccomp, AppArmor, capabilities Linux, hostPath et comptes de service
- Contrôle des accès : utilisateurs, rôles, RoleBinding
- Pod Security Standards et Pod Security Admission : profils Privileged, Baseline et Restricted
- Chiffrement de données sensibles (secrets, etcd)

Réseau, CNI et Service Mesh

- Politique réseau native (NetworkPolicy)

- Plugins CNI : Calico, Cilium, etc.
- Sécurisation des communications entre workloads : NetworkPolicy, chiffrement et mTLS
- Visibilité via eBPF

Exemples de travaux pratiques (à titre indicatif) :
Déploiement d'une application multipods
Création de NetworkPolicies pour interdire certains flux
Intégration d'un microservice dans Istio
Gestion TLS, routage, jaeger/grafana pour visualisation

Jour 2 – Après-midi
Conformité, sécurité dynamique et politiques avancées
Écosystème CNCF et outils de sécurité

- CNCF : Falco, Kyverno, OPA, Kubesploit, Kube-Bench
- Chaîne de sécurité des artefacts (supply chain)
- Cas d'usage : détection, prévention, audit

Déploiement et gestion de politiques avancées

- Signature et vérification d'image avec Cosign
- Politiques Kyverno : forcer labels, registres, contraintes
- Sécurité dynamique : règles de surveillance personnalisées

Exemples de travaux pratiques (à titre indicatif) :
Déploiement Falco et personnalisation des règles
Création de politiques Kyverno : forcer un registre, limites CPU/mémoire
Déploiement de Cosign avec Harbor pour signer et vérifier les images
Sécurisation du CoreDNS
Gestion automatisée des secrets et LimitRanges

Méthodes pédagogiques

- Ce cours se présente sous la forme d'un séminaire ponctué de démonstration afin d'illustrer les concepts théoriques abordés.

- Le formateur tient compte de la situation de chaque apprenant et se base sur les expériences, les connaissances et les questions particulières des participants pour nourrir le groupe de cas concrets et de retours d'expériences ciblées

Les supports de formation seront les suivants :

- Présentation théorique au format pdf

Ces supports seront fournis aux participants au cours de la formation au format PDF.

Méthodes d'évaluation des acquis

Avant la formation :

- Le questionnaire de positionnement et d’auto-évaluation des compétences adapté à la formation :
    - Complété individuellement par chaque stagiaire avant la formation
    - Permet de recueillir et de mettre à disposition du formateur avant la formation

En cours de formation :

- Points d’étapes réguliers par le formateur sur la compréhension des stagiaires, de la réponse de la formation à leurs attentes et à leurs besoins
- Retour d’expérience en fin de journée de formation pour ajustements éventuels de la suite de la formation.

Après la formation « à chaud » :

- Le questionnaire d’auto-évaluation des compétences complété individuellement par chaque stagiaire après la formation et ajusté (si besoin) puis validé par le formateur en fonction des évaluations réalisées en cours de formation.
- Le questionnaire de satisfaction « à chaud » complété individuellement par chaque stagiaire en fin de formation.
- Le compte rendu formateur complété par le formateur.

Après la formation « à froid » :

Le questionnaire de satisfaction « à froid » complété individuelle par chaque stagiaire quelques semaines après la session de formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.