

# Formation **Kubernetes and Cloud Native Security Associate** (préparation à la certification **KCSA**)

Cette formation prépare à la certification Kubernetes and Cloud Native Security Associate (KCSA). Elle s'adresse aux personnes souhaitant acquérir ou consolider les connaissances fondamentales en sécurité dans l'écosystème cloud natif, avec un focus particulier sur Kubernetes.

## **Durée**

2 jours

## **Objectifs pédagogiques**

- ❖ Expliquer les principes et concepts clés de la sécurité cloud native
- ❖ Décrire le rôle et les enjeux de sécurité des principaux composants d'un cluster Kubernetes
- ❖ Mettre en œuvre les fondamentaux de la sécurité Kubernetes
- ❖ Analyser un modèle de menace Kubernetes en identifiant les frontières de confiance, les flux de données et les principaux scénarios d'attaque
- ❖ Renforcer la sécurité de la plateforme Kubernetes et du socle cloud natif
- ❖ Situer Kubernetes dans les cadres de conformité et de threat modelling pertinents, et utiliser l'automatisation et les outils associés pour adresser la conformité

## **Public**

Ingénieurs devops, sysadmins, architectes...

## **Prérequis**

Pour suivre cette formation dans de bonnes conditions, il est recommandé de :

- Avoir des connaissances de base sur Kubernetes (ressources principales, fonctionnement général d'un cluster).
- Comprendre les notions fondamentales du cloud et des conteneurs (images, registres, réseau, principes de sécurité de haut niveau).

## Programme de formation

### Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

### Vue d'ensemble de la sécurité cloud native

Les 4C de la sécurité cloud native  
Sécurité du fournisseur cloud et de l'infrastructure  
Contrôles de sécurité et cadres de référence  
Techniques d'isolation  
Sécurité des dépôts d'artefacts et des images  
Sécurité des workloads et du code applicatif

### Sécurité des composants du cluster Kubernetes

Sécurité du serveur d'API (API Server)  
Sécurité du Controller Manager  
Sécurité du Schedule  
Sécurité de Kubelet  
Sécurité du runtime de conteneurs  
Sécurité de kube-proxy  
Sécurité des Pods  
Protection et sécurisation d'etcd  
Sécurité du réseau de conteneurs  
Sécurité côté client  
Sécurité du stockage

### Fondamentaux de la sécurité Kubernetes

Pod Security Standards  
Pod Security Admissions  
Authentification  
Autorisation

### Gestion des secrets

Isolation et segmentation  
Journalisation d'audit  
Network Policies

### Modèle de menace Kubernetes

Frontières de confiance Kubernetes et flux de données  
Mécanismes de persistance de l'attaquant  
Attaques par déni de service (DoS)  
Exécution de code malveillant et compromission d'applications en conteneurs  
Attaquant présent sur le réseau  
Accès à des données sensibles  
Escalade de privilèges

### Sécurité de la plateforme

Sécurité de la supply chain  
Sécurité et gestion des registres d'images  
Observabilité et sécurité  
Service mesh et contrôles de sécurité associés  
PKI et gestion des certificats  
Connectivité et sécurisation des communications  
Admission control

### Conformité et cadres de sécurité

Cadres de conformité en sécurité cloud native  
Cadres de threat modelling  
Conformité de la supply chain  
Automatisation et outillage pour la sécurité et la conformité

## Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

## Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.
- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.
- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.