

Certifiante Sessions garanties disponibles

Formation Certified Kubernetes Security Specialist (préparation à la certification CKS)

Réf. SF34008

Obtenez toutes les clés pour passer l'examen de certification CKS grâce à notre formation de 2 jours !

2 j Durée	1 600 € HT Inter / participant	4 000 € HT Intra (≤12 pers.)	9 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Se préparer efficacement au passage de l'examen de certification CKS
- ✓ Mettre en œuvre les meilleures pratiques pour se prémunir contre les menaces à travers l'infrastructure physique, les applications, les réseaux, les données, les utilisateurs et les charges de travail
- ✓ Démontrer une expertise dans la sécurisation des applications basées sur des conteneurs et des plateformes Kubernetes
- ✓ Détecter les failles de sécurité potentielles, identifier les phases d'attaque et les acteurs malveillants dans l'environnement, et garantir des mesures de sécurité robustes à chaque étape de l'opération à travers l'ensemble du cycle de développement

Public visé & prérequis

- Public visé** Administrateurs systèmes et réseaux, Architectes techniques, Ingénieurs DevOps
- Prérequis** Être titulaire de la certification CKA, Certified Kubernetes Administrator. Avoir de bonnes connaissances sur les systèmes Unix et les conteneurs, ainsi qu'une expérience de travail significative avec Kubernetes pour l'administration.

Programme détaillé

Configuration du cluster

Utiliser les politiques de sécurité du réseau pour restreindre l'accès au niveau du cluster
Utiliser le benchmark CIS pour examiner la configuration de sécurité des composants Kubernetes (etcd, kubelet, kubedns, kubeapi)
Configurer correctement les objets Ingress avec un contrôle de sécurité
Protéger les métadonnées des nœuds et les endpoints
Minimiser l'utilisation et l'accès aux éléments de l'interface graphique
Vérifier les binaires de la plateforme avant de les déployer

Cluster Hardening

Restreindre l'accès à l'API de Kubernetes
Utiliser des contrôles d'accès basés sur les rôles pour minimiser l'exposition
Faire preuve de prudence dans l'utilisation des comptes de service, par exemple en désactivant les valeurs par défaut, en minimisant les autorisations sur les comptes nouvellement créés
Mettre à jour Kubernetes fréquemment

System Hardening

Minimiser l'empreinte du système d'exploitation hôte (réduire la surface d'attaque)
Minimiser les rôles IAM
Minimiser l'accès externe au réseau
Utiliser de manière appropriée les outils de durcissement du noyau tels que AppArmor, seccomp

Minimiser les vulnérabilités des microservices

Configurer des domaines de sécurité appropriés au niveau du système d'exploitation

Gérer les secrets Kubernetes

Utiliser des bacs à sable d'exécution de conteneurs dans les environnements multi-tenants (par exemple, gvisor, conteneurs kata).

Mettre en œuvre le chiffrement de pod à pod par l'utilisation de mTLS

Sécurité de la Supply Chain

Minimiser l'empreinte de l'image de base

Sécurisez votre chaîne d'approvisionnement : établissez une liste blanche des registres autorisés, signez et validez les images.

Utilisez l'analyse statique des charges de travail des utilisateurs (par exemple, ressources Kubernetes, fichiers Docker).

Analyser les images pour détecter les vulnérabilités connues

Surveillance, journalisation et sécurité d'exécution

Effectuer des analyses des processus syscall et des activités de fichiers au niveau de l'hôte et du conteneur pour détecter les activités malveillantes.

Détecter les menaces au sein de l'infrastructure physique, des applications, des réseaux, des données, des utilisateurs et des charges de travail.

Détecter toutes les phases de l'attaque, indépendamment de l'endroit où elle se produit et de la manière dont elle se propage.

Effectuer des recherches analytiques approfondies et identifier les mauvais acteurs au sein de l'environnement.

Garantir l'immuabilité des conteneurs au moment de l'exécution.

Utiliser les journaux d'audit pour surveiller l'accès.

Prochaines sessions

DATE	LIEU	STATUT
02/11/2026	Paris	Sur confirmation
02/11/2026	à distance	Session garantie
02/11/2026	Lille	Sur confirmation
02/11/2026	Nantes	Sur confirmation
10/12/2026	Lyon	Sur confirmation
10/12/2026	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Conteneurs & Orchestration (Cloud Native) : 4,9/5 — 75 avis

Julien J. — Formateur compétent et programme adapté à notre besoin.

Dorian B. — Formateur à l'écoute, curieux et qui livre des retours d'expériences intéressants.

Votre formateur

Fabrice J. — Formateur Kubernetes

Fabrice intervient sur des formations portant sur les conteneurs et l'orchestration cloud native. Les sujets abordés incluent notamment Kubernetes. Son activité de formation remonte à 2017.

Ils nous font confiance

Cette année notre filière Conteneurs & Orchestration (Cloud Native) a accompagné plus de 157 entreprises dont :

SOPRA STERIA AMADEUS DATA PROCESSING GMBH LBC FRANCE MALAKOFF HUMANIS AMAP STMICROELECTRONICS FRANCE TRAVAIL SQLI
ALSTOM AMADEUS CLARANET +147 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com