Kubernetes — Sécurité avancée et hardening (CKS)

Lien : https://innov-systems.com/formation/kubernetes-securite-avancee-et-hardening-cks

DURÉE
5 jours (35h)

RÉFÉRENCE
VSC397

CATÉGORIE
Kubernetes

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes avancés de sécurité Kubernetes (CKS)
- Sécuriser l’ensemble d’un cluster Kubernetes en production
- Appliquer les bonnes pratiques de hardening du control plane
- Mettre en place RBAC et politiques de sécurité robustes
- Sécuriser les workloads et conteneurs
- Implémenter des Network Policies avancées
- Gérer les secrets de manière sécurisée
- Détecter et prévenir les vulnérabilités dans les clusters
- Sécuriser les pipelines CI/CD Kubernetes
- Renforcer la résilience des environnements cloud-native
- Préparer la certification CKS
- Étudier des cas concrets de sécurité Kubernetes

POUR QUI ?

- Ingénieurs DevOps
- SRE (Site Reliability Engineers)
- Ingénieurs Kubernetes
- Architectes cloud
- Ingénieurs sécurité cloud
- Platform engineers
- Administrateurs systèmes et réseaux
- Ingénieurs infrastructure IT
- Consultants DevSecOps
- Chefs de projet infrastructure cloud
- Experts cybersécurité
- Toute personne impliquée dans la sécurisation des environnements Kubernetes

Innov Systems

Programme détaillé

1 / Introduction à la sécurité Kubernetes (CKS)

- Présentation de la certification CKS (Certified Kubernetes Security Specialist)
- Enjeux de sécurité des clusters Kubernetes
- Surface d’attaque dans les environnements cloud-native

2 / Modèle de sécurité Kubernetes

- Authentification, autorisation et admission control
- RBAC (Role-Based Access Control)
- Séparation des responsabilités et multi-tenancy

3 / Sécurisation du cluster Kubernetes

- Hardening du control plane
- Sécurisation de etcd
- Protection des API servers

4 / Sécurité des workloads

- Security Context et Pod Security Standards
- Restriction des privilèges (non-root, capabilities)
- Isolation des conteneurs

5 / Network security avancée

- Network Policies et segmentation réseau
- Zero Trust networking dans Kubernetes
- Protection des flux est-ouest

Innov Systems

6 / Sécurisation des images conteneurs

- Scan des vulnérabilités d’images
- Signature et vérification des images
- Gestion des registries sécurisés

7 / Secrets management

- Kubernetes Secrets et limites
- Intégration avec Vault et solutions externes
- Chiffrement des secrets at-rest et in-transit

8 / Audit et observabilité sécurité

- Audit logs Kubernetes
- Détection des comportements suspects
- Intégration avec SIEM et SOC

9 / Supply chain security

- Sécurisation des pipelines CI/CD
- Politique de déploiement sécurisé
- Contrôle des dépendances et artefacts

10 / Cas pratiques et hardening en production

- Mise en œuvre d’un cluster sécurisé
- Tests de conformité et audit CKS
- Bonnes pratiques de production Kubernetes

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés