Sécurité Kubernetes — Hardening, RBAC, Network Policies et Pod Security

Lien : https://innov-systems.com/formation/securite-kubernetes-hardening-rbac-network-policies-et-pod-security

DURÉE
5 jours (35h)

RÉFÉRENCE
SI77

CATÉGORIE
DevSecOps et Sécurité CI/CD

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes de sécurité Kubernetes
- Mettre en œuvre le RBAC de manière sécurisée
- Appliquer les Pod Security Standards
- Configurer des Network Policies efficaces
- Sécuriser les accès au cluster Kubernetes
- Durcir les nœuds et le control plane
- Protéger les workloads conteneurisés
- Gérer les secrets et les identités de manière sécurisée
- Déployer des clusters Kubernetes conformes aux bonnes pratiques
- Mettre en place des stratégies d’audit et de monitoring
- Réduire les risques de compromission des clusters
- Étudier des cas concrets de sécurisation Kubernetes

POUR QUI ?

- DevOps Engineers
- SRE (Site Reliability Engineers)
- Cloud Engineers
- Kubernetes Administrators
- Platform Engineers
- Security Engineers
- DevSecOps Engineers
- Architectes Cloud
- Administrateurs systèmes
- Ingénieurs infrastructure
- Consultants cybersécurité
- Toute personne impliquée dans l’exploitation et la sécurisation de Kubernetes

Innov Systems

Programme détaillé

1 / Introduction à la sécurité Kubernetes

- Enjeux de sécurité des clusters Kubernetes en production
- Modèle de sécurité natif Kubernetes
- Menaces et surfaces d’attaque principales

2 / Architecture de sécurité Kubernetes

- Control plane et worker nodes sécurisés
- API Server et mécanismes d’authentification
- Sécurisation des communications internes

3 / RBAC (Role-Based Access Control)

- Principes du contrôle d’accès basé sur les rôles
- Roles, ClusterRoles, RoleBindings
- Gestion fine des permissions utilisateurs et services

4 / Authentification et autorisation

- Méthodes d’authentification (certificats, tokens, OIDC)
- Gestion des comptes utilisateurs et service accounts
- Politiques d’accès granulaires

5 / Pod Security Standards (PSS)

- Remplacement des PodSecurityPolicies (PSP)
- Profils : privileged, baseline, restricted
- Durcissement des workloads conteneurisés

Innov Systems

6 / Network Policies

- Isolation réseau entre pods
- Contrôle du trafic entrant et sortant
- Micro-segmentation des services Kubernetes

7 / Sécurisation des images et supply chain

- Scanning des images conteneurisées
- Signature et vérification des images
- Utilisation de registries sécurisés

8 / Sécurité du cluster et hardening

- Sécurisation du kubelet et des nodes
- Chiffrement des secrets Kubernetes
- Gestion sécurisée des etcd

9 / Monitoring et audit de sécurité

- Audit logs Kubernetes
- Détection d’anomalies et intrusion
- Intégration avec SIEM et outils de sécurité

10 / Bonnes pratiques et cas pratiques

- Hardening complet d’un cluster Kubernetes
- Mise en place de politiques de sécurité avancées
- Études de cas en environnement production

Inov 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