Sécurité des conteneurs et orchestrateurs (Docker, Kubernetes) : de la configuration au runtime

Lien : https://innov-systems.com/formation/securite-des-conteneurs-et-orchestrateurs-docker-kubernetes-de-la-configuration-au-runtime

DURÉE
5 jours (35h)

RÉFÉRENCE
SI79

CATÉGORIE
DevSecOps et Sécurité CI/CD

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques liés aux conteneurs et à Kubernetes
- Sécuriser les images, registries et pipelines CI/CD
- Durcir la configuration Docker et Kubernetes
- Mettre en place des politiques RBAC et Network Policies
- Protéger les secrets et identités des workloads
- Déployer des outils de détection runtime (Falco, etc.)
- Appliquer les bonnes pratiques CIS Benchmarks
- Intégrer la sécurité dans le cycle DevOps (DevSecOps)
- Surveiller et auditer les clusters Kubernetes
- Réduire la surface d’attaque des environnements cloud-native
- Assurer la conformité des infrastructures conteneurisées
- Étudier des cas concrets de sécurisation Kubernetes en production

POUR QUI ?

- DevSecOps engineers
- Kubernetes administrators
- Cloud security engineers
- Platform engineers
- DevOps engineers
- Security engineers
- Software engineers cloud-native
- SRE (Site Reliability Engineers)
- Architectes cloud
- SOC analysts
- Consultants cybersécurité
- Toute personne impliquée dans la sécurité des environnements conteneurisés

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des conteneurs et de Kubernetes

- Principes de la conteneurisation (Docker, OCI)
- Architecture Kubernetes et surface d’attaque
- Enjeux de sécurité cloud-native

2 / Sécurisation des images de conteneurs

- Construction d’images sécurisées
- Réduction de la surface d’attaque (minimal base images)
- Scanning des vulnérabilités (Trivy, Clair)

3 / Gestion des registres de conteneurs

- Sécurisation des registries (Docker Hub, private registries)
- Signature et vérification des images (Notary, Cosign)
- Contrôle d’accès aux artefacts

4 / Sécurité de la configuration Docker

- Docker daemon security
- Namespaces, cgroups et isolation
- Bonnes pratiques de configuration sécurisée

5 / Sécurité du cluster Kubernetes

- Hardening du control plane
- Sécurisation etcd et API Server
- Gestion des RBAC Kubernetes

Innov Systems

6 / Network security dans Kubernetes

- Network Policies et segmentation des pods
- Service Mesh (Istio, Linkerd) et sécurité mTLS
- Protection des communications internes

7 / Gestion des secrets et des identités

- Kubernetes Secrets et alternatives sécurisées (Vault)
- Rotation et chiffrement des secrets
- Identity management pour workloads

8 / Sécurité runtime des conteneurs

- Détection des comportements anormaux (Falco)
- Runtime protection et sandboxing
- Monitoring des workloads en production

9 / Compliance et gouvernance cloud-native

- CIS Benchmarks pour Docker et Kubernetes
- Politiques de sécurité et admission controllers
- Audit et conformité continue

10 / DevSecOps et sécurisation du pipeline CI/CD

- Intégration de la sécurité dans les pipelines
- Scanning des dépendances et images
- Automatisation des contrôles de sécurité

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

08 au 12 Fév. 2027	Présentiel - Casablanca
05 au 09 Avr. 2027	Présentiel - Casablanca
31 Mai au 04 Juin 2027	Présentiel - Casablanca
26 au 30 Juil. 2027	Présentiel - Casablanca
20 au 24 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