Container Security — Scanning, runtime protection et compliance (Trivy, Falco)

Lien : https://innov-systems.com/formation/container-security-scanning-runtime-protection-et-compliance-trivy-falco

DURÉE
5 jours (35h)

RÉFÉRENCE
SI74

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 Kubernetes
- Maîtriser l’analyse de vulnérabilités avec Trivy
- Mettre en place une sécurité runtime avec Falco
- Sécuriser les pipelines CI/CD de conteneurs
- Appliquer les bonnes pratiques de durcissement Kubernetes
- Gérer les vulnérabilités et leur remédiation
- Mettre en conformité les environnements containerisés
- Intégrer la sécurité dans la supply chain logicielle
- Détecter les comportements anormaux en production
- Automatiser les contrôles de sécurité des images
- Renforcer la sécurité des workloads cloud-native
- Étudier des cas concrets d’attaques et de protection conteneurisée

POUR QUI ?

- DevSecOps Engineers
- DevOps Engineers
- Cloud Engineers
- Kubernetes Administrators
- SRE (Site Reliability Engineers)
- Security Engineers
- Platform Engineers
- Software Engineers
- Infrastructure Engineers
- SOC Analysts
- Consultants cybersécurité
- Toute personne impliquée dans la sécurité des conteneurs et Kubernetes

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des conteneurs

- Enjeux de sécurité dans les environnements containerisés
- Surface d’attaque des conteneurs et orchestration Kubernetes
- Principes de sécurité cloud-native

2 / Architecture de sécurité des conteneurs

- Image layers et risques associés
- Runtime container et isolation
- Chaîne CI/CD et exposition des vulnérabilités

3 / Scanning des images de conteneurs avec Trivy

- Analyse des vulnérabilités dans les images Docker
- Détection des CVE dans les dépendances
- Intégration de Trivy dans les pipelines CI/CD

4 / Gestion des vulnérabilités et remediation

- Priorisation des failles critiques
- Patch management des images containerisées
- Politique de mise à jour des images

5 / Runtime security avec Falco

- Détection d’anomalies en temps réel
- Surveillance des comportements système
- Règles de détection des menaces

Innov Systems

6 / Sécurisation des workloads Kubernetes

- Pod security standards
- RBAC et contrôle d’accès
- Network policies et segmentation

7 / Compliance et durcissement des environnements

- Benchmarks CIS Docker et Kubernetes
- Conformité réglementaire et sécurité interne
- Audit des environnements containerisés

8 / Supply chain security pour conteneurs

- Signature d’images et provenance
- Registry sécurisé (Docker Registry, Harbor)
- SBOM pour images containerisées

9 / Monitoring et réponse aux incidents

- Logs et alerting sécurité
- Intégration avec SIEM
- Gestion des incidents de sécurité container

10 / Cas pratiques et déploiement sécurisé

- Mise en place d’un pipeline sécurisé de conteneurs
- Détection d’attaques runtime en direct
- Bonnes pratiques en 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

18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca
30 Août au 03 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