KUBERNETES SÉCURISER VOTRE PLATEFORME

Public	Administrateurs systèmes, DevOps, DevSecOps, développeurs et/ou architectes.
Durée	2 jours - 14 heures
Pré-requis	voir des connaissances de base en administration Linux/Unix, sur Docker et les principes de fonctionnement des conteneurs, et sur Kubernetes et les principes de fonctionnement des ressources basiques.
Objectifs	Déterminer les bonnes pratiques de sécurité dans Kubernetes Configurer et utiliser des outils de sécurisation du registre Paramétrer et utiliser des outils de conformité Configurer et utiliser des outils de sécurité en temps réel Mettre en place des stratégies de sécurité dans Kubernetes.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

LES CONCEPTS DE LA SÉCURITÉ NATIVE KUBERNETES

- Que doit-on sécuriser dans Kubernetes ?
- Quelques exemples d'attaques connues dans l'écosystème Docker / Kubernetes
- Vulnérabilités et vecteurs d'attaques
- Gestion des accès : qu'est-ce que le RBAC (Role Based Access Control) ?
- La gestion des certificats
- Fonctionnement des contrôleurs d'admission
- Sécurisation des accès aux composants
- Chiffrement de données dans Kubernetes

SÉCURITÉ CONTINUE DES IMAGES

- Quels risques encourt-on ?
- Comment sécuriser un registre d'image ?
- Quelles sont les sources de vulnérabilité à utiliser ?
- Quels sont les possibilités offertes par la CI/CD ?
- Existe-t-il des solutions propriétaires ? Quels bénéfices ?
- Quelles sont les meilleures pratiques dans la gestion des environnements et la promotion des images ?
- Découverte des outils Open Source Harbor, Clair et Notary

CONFORMITÉ DE KUBERNETES

- Qu'est-ce que la conformité ?
- Quels risques encourt-on ?
- Quelles sont les bonnes pratiques à adopter ?
- Comment s'assurer de la conformité de son infrastructure ?
- Comment gérer le cycle de vie des clés ?
- Existe-t-il des solutions propriétaires ? Quels bénéfices ?
- Découverte du projet Open Policy Agent

SÉCURISATION EN TEMPS RÉEL

- Qu'est-ce que la sécurisation en temps réel d'une infrastructure Kubernetes ?
- Quels risques encourt-on ?
- Comment contrôler continuellement son infrastructure Kubernetes ?
- Monitoring, Logging et Chaos Engineering : quels bénéfices pour la sécurité ?
- Existe-t-il des solutions propriétaires ? Quels bénéfices ?
- Découverte du projet Falco

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 29/09/2023

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères : Expérience, pédagogie, dynamisme et prévoyance.