Développez vos talents
Certifiez vos compétences

Cloud privé et hybride / Multi-Cloud

Kubernetes - Sécuriser votre plateforme

2 jours (14h00) | ★★★★½ 4,6/5 | KUB-SEC | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cloud › Cloud privé et hybride / Multi-Cloud

À l'issue de ce stage vous serez capable de :

- 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.

Niveau requis

Avoir 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.

Public concerné

Administrateurs systèmes, DevOps, DevSecOps, développeurs et/ou architectes.

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 M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (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.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Les concepts de la sécurité native Kubernetes

- Que doit-on sécuriser dans Kubernetes ?
  - Moteur
  - Conteneur
  - Réseau
  - Secret
- 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

Exemples de travaux pratiques (à titre indicatif)

- *Sécurisation du cluster (RBAC, chiffrement, sécurisation du réseau)*
- *Tour d'horizon des solutions de sécurité autour de l'écosystème 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

Exemples de travaux pratiques (à titre indicatif)

- *Installation et manipulation des projets Harbor, Clair et Notary*
  - *Mise en situation avec injection d'images dangereuses et tentative de récupération d'image non signée*

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

Exemples de travaux pratiques (à titre indicatif)

- *Installation et manipulation du projet Open Policy Agent*
  - *Mise en situation avec tentative d'injection d'image non conforme*

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

Exemples de travaux pratiques (à titre indicatif)

- *Installation et manipulation du projet Falco*
  - *Mise en situation avec tentative d'élévation de privilège, modification de conteneur et actions non désirées*

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)