Kubernetes – Sécurité

La formation "Kubernetes – sécurité" est spécialement conçue pour les professionnels de l'IT souhaitant **approfondir leurs connaissances en sécurisation des environnements Kubernetes.** Au cours de cette formation, vous découvrirez les meilleures pratiques de sécurité, de la configuration des outils de sécurisation des registres à l'utilisation des outils de conformité et de sécurité en temps réel. Vous apprendrez à mettre en place des stratégies de sécurité robustes dans Kubernetes, couvrant tous les aspects nécessaires pour protéger vos applications et infrastructures.

La formation est structurée sur deux journées intensives : la première journée se concentre sur les principes technologiques des conteneurs et la sécurité, allant de Docker à l'OCI, tandis que la deuxième journée aborde la sécurité et l'orchestration avec Kubernetes ainsi qu'un tour d'horizon des pure-players de la sécurité des conteneurs.

Vous bénéficierez d'un programme détaillé couvrant les fondamentaux des conteneurs, les menaces spécifiques, la sécurisation des moteurs de conteneurs, et les évolutions technologiques vers des modèles de containers microVM et unikernels. Rejoignez-nous pour maîtriser les enjeux de la sécurité dans Kubernetes et assurer la protection optimale de vos environnements Cloud Native.

LES INFORMATIONS PRATIQUES :

- 2 jours soit 14 heures
- 1690€ HT / stagiaire
- En présentiel ou classe à distance

Objectifs de la formation :

- Appréhender les bonnes pratiques de sécurité dans Kubernetes
- Configurer et utiliser des outils de sécurisation du registre
- Configurer 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

Prérequis :

- Avoir des connaissances de base en administration Linux / Unix, sur Docker, sur les principes de fonctionnement des conteneurs ainsi que sur le réseau SDN
- Avoir suivi la formation KUB-ORCH-CON "Kubernetes - Orchestrer ses conteneurs" ou avoir les connaissances équivalentes
- Avoir suivi la formation KUB-PRAT-AV "Kubernetes – Pratiques avancées" ou avoir les connaissances équivalentes

Public concerné :

Administrateurs systèmes, Devops, DevSecOps, Développeurs, Architecte, SRE

Méthodologie :

- Accompagnement théorique et pratique avec une pédagogie traditionnelle alliant théorie, démonstrations et/ou exercices puis mise en pratique des notions abordées avec une évaluation des travaux pratiques réalisés.
- Le formateur tient compte de la situation de chaque apprenant et se base sur les expériences, les connaissances et les questions particulières des participants pour nourrir le groupe de cas concrets et de retours d'expériences ciblées

Méthode d'évaluation de l'acquisition des compétences :

- **Avant la formation :**
  - Le questionnaire de positionnement et d'auto-évaluation des compétences adapté à chaque formation :

        - Complété individuellement par chaque stagiaire avant la formation
        - Permet de recueillir et de mettre à disposition du formateur avant la formation

- **En cours de formation :**
    - Points d'étapes réguliers par le formateur sur la compréhension des stagiaires, de la réponse de la formation à leurs attentes et à leurs besoins
    - Retour d'expérience en fin de journée de formation pour ajustements éventuels de la suite de la formation.

- **Après la formation « à chaud » :**
    - Le questionnaire d'auto-évaluation des compétences complété individuellement par chaque stagiaire après la formation et ajusté (si besoin) puis validé par le formateur en fonction des évaluations réalisées en cours de formation.
    - Le questionnaire de satisfaction « à chaud » complété individuellement par chaque stagiaire en fin de formation.
    - Le bilan du formateur complété par le formateur.

- **Après la formation « à froid » :**
    - Le questionnaire de satisfaction « à froid » complété individuelle par chaque stagiaire quelques semaines après la session de formation.

Modules de formation :

1ère journée :

- Module 1 – Containers - principes technologiques
- Module 2 – Sécurité - de Docker à l'OCI

2ème journée :

- Module 3 – Sécurité et orchestration avec Kubernetes
- Module 4 – Les pure-players de la sécurité des containers

Modalités de formation :

ILKI Academy propose et adapte ses formations en s'appuyant sur l'une ou plusieurs modalités parmi les suivantes :

- **Formation en présentiel :**
  - Cette modalité implique des sessions de formation organisées dans des lieux physiques où les formateurs et les participants se réunissent en personne.
  - Elle favorise les interactions directes, les discussions en face-à-face et les activités pratiques.
  - Les avantages incluent le renforcement des liens sociaux, la rétroaction instantanée et la possibilité pour les participants de poser des questions en temps réel.
- **Formation en distanciel :**
  - Cette méthode pédagogique se déroule à distance, souvent via des plateformes en ligne, des visioconférences ou des modules e-learning.
  - Les formateurs utilisent des outils de communication numériques pour dispenser les cours, interagir avec les apprenants, répondre aux questions et fournir un retour d'information.
  - Cette méthode offre une plus grande flexibilité en termes de planification et d'accès à la formation, ce qui est particulièrement utile pour les personnes ayant des contraintes de temps et/ou de déplacement.
- **Formation hybride :**
  - La formation hybride combine des éléments des deux modalités précédentes, en intégrant à la fois des sessions en présentiel et des composantes à distance.
  - Les participants peuvent suivre une partie de la formation en personne et une partie à distance, souvent à travers des modules en ligne ou des ressources numériques.
  - Cette approche offre la flexibilité de l'apprentissage en ligne tout en permettant des interactions en face-à-face lors des sessions en personne, offrant ainsi une expérience d'apprentissage complète et adaptable.

Modalités d'évaluation

Avant la formation :

Le questionnaire de positionnement et d'auto-évaluation des compétences adapté à chaque formation :

- Complété individuellement par chaque stagiaire avant la formation
- Permet de recueillir et de mettre à disposition du formateur avant la formation :
    - Le niveau de chaque stagiaire pour chaque objectif de formation
    - Les attentes spécifiques de chaque stagiaire pour chaque objectif de la formation
    - Les demandes d'éventuelles adaptations de contenus à des contextes spécifiques

En cours de formation :

- Points d'étapes réguliers par le formateur sur la compréhension des stagiaires, de la réponse de la formation à leurs attentes et à leurs besoins
- Retour d'expérience en fin de journée de formation pour ajustements éventuels de la suite de la formation
- Evaluation des acquis des stagiaires via des quizz, des questions et la vérification de la bonne réalisation des cas d'études et des travaux pratiques.

Après la formation « à chaud » :

Le questionnaire d'auto-évaluation des compétences adapté à chaque formation :

- Complété individuellement par chaque stagiaire après la formation
- Permet d'évaluer en fin de formation la progression de chaque stagiaire sur chaque objectif de formation
- Questionnaire ajusté (si besoin) et validé par le formateur en fonction des évaluations réalisées en cours de formation

Le questionnaire de satisfaction « à chaud » :

- Complété en fin de formation, il permet de recueillir les impressions et les réactions des stagiaires en fin de session notamment sur la qualité du contenu, la réponse aux attentes, la qualité de la pédagogie et de l'animation et les propositions d'axes d'améliorations
- Permet de mesure la qualité perçue de chaque formation par l'ensemble des stagiaires

Le bilan du formateur :

- Permet au formateur de réfléchir de manière rétrospective sur le déroulement de la formation, afin d'évaluer son efficacité et d'identifier les points forts ainsi que les axes d'amélioration

Equipements nécessaires pour la formation :

- **Equipements pédagogiques :**

  - Vidéoprojecteur : oui
  - Autres : paperboard, tableau blanc et/ou tableau interactif

- **Equipements informatiques :**

  - Configuration des stations de travail :
    - ✓ Processeur (minimum) : Intel i5
    - ✓ Mémoire (minimum) : 8 Go
    - ✓ Stockage (minimum) 250 Go SSD
    - ✓ Réseau : haut débit filaire ou sans fil

- **Logiciels installés :**

  - Système d'exploitation : Windows 10 (ou supérieur)
  - Liste des logiciels spécifiques : Microsoft Office 365 (Teams, Word, Excel et PowerPoint)

- **Accès réseau et internet :**

  - Internet :
    - ✓ Accès non filtré à internet (http, https, SSH…)
    - ✓ Accès aux consoles de AWS, Azure et GCP
    - ✓ Téléchargement de documents depuis AWS S3
    - ✓ Accès distant SSH à des serveurs

  - Droits sur les stations de travail :
    - ✓ Droits du formateur : administrateur local
    - ✓ Droits des stagiaires : administrateur local

- **Accès cloud providers :**

- Cloud provider : fourni par ILKI Academy

Informations pratiques

Modalités et délais d'accès :

L'accès à nos formations peut être initié, soit par l'employeur, soit à l'initiative du salarié avec l'accord de ce dernier, soit à l'initiative propre du salarié.

Pour chaque demande de formation, nous réalisons un entretien téléphonique ou un échange via mail ou en présentiel, afin d'établir, si besoin, une formation personnalisée tenant compte de vos attentes, de vos préférences et de vos contraintes.

Une proposition commerciale ainsi qu'un programme adapté vous seront transmis à la suite de l'entretien.

A réception du devis signé l'organisation logistique, technique, pédagogique et financière est établie.

Le délai d'accès aux formations tient compte de ces différentes formalités afin d'être accessible dans un temps minimum de trois semaines avant le début de l'action de formation.

Contacts :

Linda BOUROUROU
Chargée d'affaires
Tél : +33 (0)6 45 10 18 69
formation@ilki.fr

Accessibilité aux personnes handicapées :

Lors de l'inscription à nos formations, nous étudions avec vous et à travers un questionnaire les différents aménagements et adaptations que nous pouvons mettre en œuvre pour favoriser votre apprentissage.

Pour cela, nous pouvons également nous appuyer sur un réseau de partenaires nationaux préalablement identifiés.

Si vous êtes en situation de handicap, merci de contacter notre référent handicap par mail à handicap@ilki.fr.

Direction Pédagogie et Qualité :	Direction Technique :	Chargée de Mission Formation et Vie des Stagiaires :
Didier MEIER	Adrien HUERRE	Linda BOUROUROU

Programme :

Containers – principes technologiques

- Les fondamentaux :
  - Évolution du niveau d'abstraction
  - Caractéristiques et format immuable du container
  - Les risques et menaces

- Sécurité des technologies sous-jacentes
  - Le rôle des namespaces
  - Le rôle des Control Groups
  - Sécurité des OS pour containers

Sécurité - de Docker à l'OCI

- La sécurité des moteurs de containers
  - Docker engine
  - Sécuriser le daemon Docker, best practices
  - Sécurité des images
  - Évolution du Docker Engine vers containerd/runc
  - Bonnes pratiques – Dockerfile
  - La sécurité sur le registre avec le scan et la signature

- Les autres acteurs de l'OCI
  - OCI Open Container Initiative
  - Impact de l'OCI sur l'écosystème
  - Évolution de la distribution des images et artefact
  - Évolution vers un modèle de containers microVM
  - Vers les Unikernels ?

Sécurité et orchestration avec Kubernetes

- Orchestration avec Kubernetes
  - Sécurité d'un environnement CaaS
  - Menaces propres à Kubernetes
  - Sécuriser le cluster
  - Contrôle des accès à l'API
  - La problématique du chiffrement

- Sécurité réseau et Service Mesh
    - Sécurité du réseau
    - Stratégies réseau Kubernetes
    - Communications containers sur K8S
    - Plugins réseaux compatibles CNI
    - Service Mesh et acteurs
    - Istio – principe de fonctionnement
    - Le développement de Ebpf
    - Bonnes pratiques pour la visibilité

- Sécurité des images
    - Sécurité du stockage des images
    - Exemple Harbor
    - Autres exemples – ECR, Azure Registry, Google Container Registry

Les pure-players de la sécurité des containers

- Tour d'horizon
    - CNCF : Cloud Native Comptuting Foundation
    - Ecosystème autour de la CNCF
    - Projets complémentaires de sécurité
    - Sécurisation des workloads et supply chain
    - Sécurité des services
    - Identité
    - Sécurité de l'environnement
    - Évolution vers la sécurité active avec Falco
    - Outils de Scan
    - Création de politiques de sécurité
    - Exemple d'outil offensif – Kubesploit
    - Conformité avec OPA – Open Policy Agent
    - Conformité avec Kyverno
    - Conformité avec Kubewarden
    - Conformité avec Kube-Bench
    - Quand utiliser ces outils ?

- Perspectives

Travaux pratiques - KUBERNETES – Sécurité

Déploiement cluster

- Déploiement d'un cluster EKS sur AWS

RBAC

- Création et configuration d'un utilisateur
- Customization du kubeconfig
- Gestion des rôles et Rolebinding
- Fédération d'identité IAM AWS

Network Policies

- Déploiement d'une application multipods
- Filtrage réseau des communications interpods
- Gestion du trafic
-

Découverte de vulnérabilités

- Récupération du certificat racine du cluster
- Exploit par port
- Exploit par kubelet
- Exploit par ETCD
- Exploit par compte compromis

Sécurité du registre

- Déploiement du registre Harbor
- Découverte des fonctionnalités de sécurité
- Filtrage par worker K8s
- Scan d'images et découverte de CVE avec Trivy
- Sécurisation des accès

Politique de sécurité avec Kyverno

- Déploiement Kyverno et Cosign
- Signature d'images avec Cosign et Harbor
- Configuration Kyverno et CoreDNS
- Création d'une politique de sécurité
- Forcer un registre spécifique
- Forcer l'utilisation d'un label

- Automatiser ses LimitRanges
- Gérer un contexte de sécurité
- Automatisation d'update et gestion

Secrets Sécurité dynamique avec Falco

- Déploiement et configuration Falco
- Découverte des règles de surveillance par défaut
- Création de règles de sécurité spécifiques
- Gestion de whitelists
- Intégration monitoring avec Prometheus

Service Mesh avec Istio

- Déploiement et utilisation de Istio
- Intégration d'une application à Istio
- Gestion de la télémétrie avec Jaeger et Grafana
- Gestion du trafic et routage dynamique
- Gestion de la sécurité avec Mutual TLS

Les retours de nos stagiaires :

Note moyenne : 4 / 5

Nombre de stagiaires formés : 7

Période : de janvier 2023 à juillet 2024