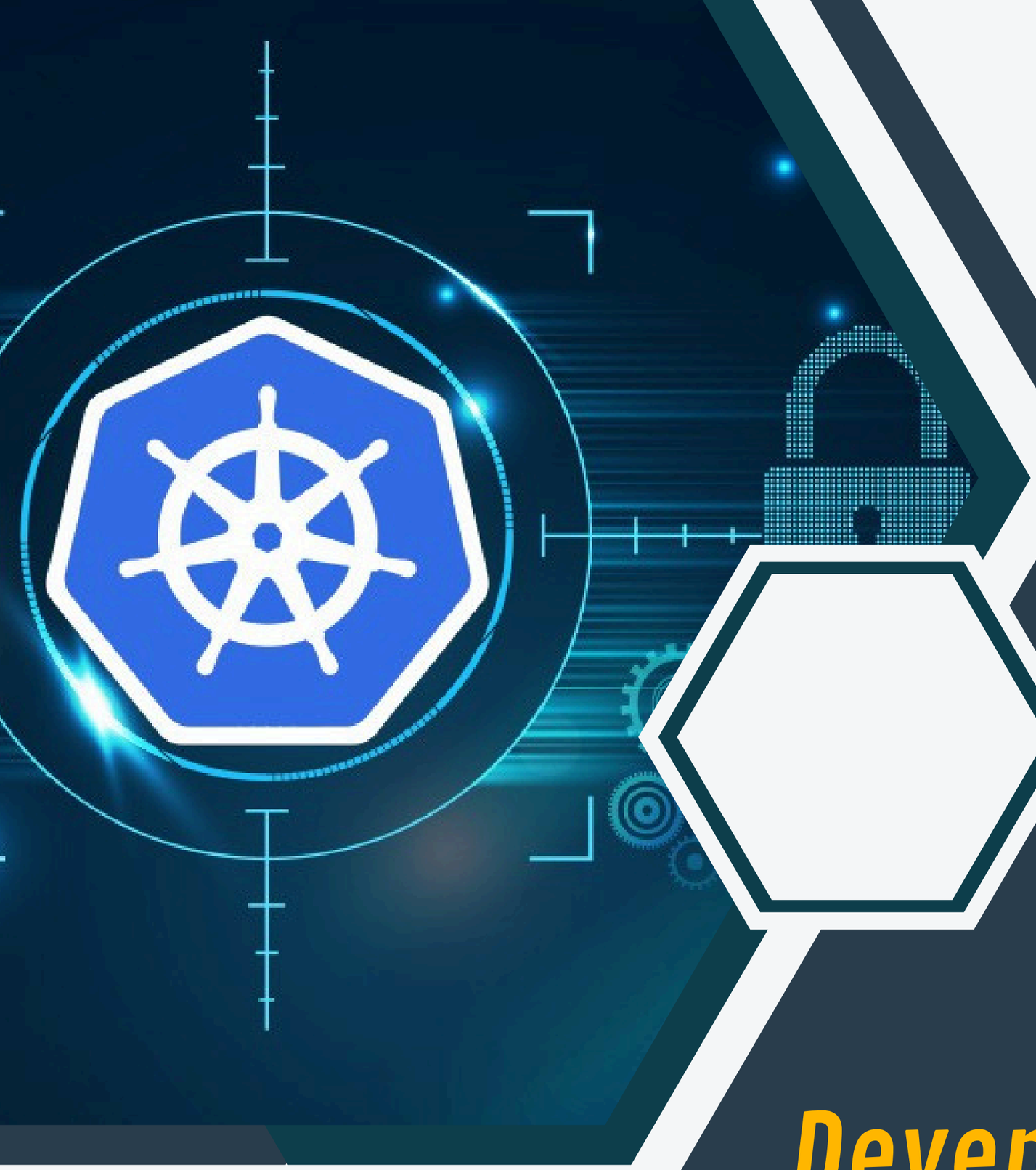

Grub-IT

un Centre de Formation Professionnel aux Métiers de l'Informatique.

- *Cloud*
- *Systèmes*
- *Réseaux*
- *Sécurité*

Devenez CKS

Sécurisez Efficacement les Clusters Kubernetes

Kube Security

Configuration

Durcissement

Supervision

Nos Contacts :

info@grub-it.com

(+237) 650 46 00 15 / 656 13 78 14

www.grub-it.com

123, Mvog-Mbi. BP 2862 Yaoundé - Cameroun

Présentation de la Formation

Ce programme couvre les aspects essentiels de la **sécurisation des clusters Kubernetes** et vous prépare la **Certification CKS (Certified Kubernetes Security Specialist)**. Il inclut la configuration sécurisée, le durcissement des clusters, la sécurisation des chaînes d'approvisionnement et la gestion des menaces.

- **Objectifs de la Formation**

Quelques uns des objectifs visés par ce cours sont :

1. **Configurer et durcir un cluster Kubernetes** pour le rendre conforme aux standards de sécurité.
2. **Mettre en place des politiques réseau** et des contrôles d'accès basés sur les rôles (RBAC)
3. **Sécuriser la chaîne d'approvisionnement** des conteneurs

- **Public Admis**

- Professionnels de la sécurité
- Administrateurs Kubernetes
- DevOps et Ingénieurs Cloud souhaitant se spécialiser dans la sécurité des clusters Kubernetes

- **Méthodes Pédagogiques**

Ce cours **dispensé en Français** est composé de :

- **Leçons** complétées par des **Démonstrations** ;
- Supports de Cours
- **Exercices**, **Travaux Pratiques** et **Laboratoires**.

Plan du Cours

Module 1 : Configuration du Cluster

1.1 : Politiques de Sécurité Réseau pour Restreindre les Accès

1.2 : Vérification des Composants Kubernetes avec les Benchmarks CIS

1.3 : Configuration Sécurisée d'Ingress avec TLS

1.4 : Protection des Métadonnées des Nœuds et des Points de Terminaison

Module 2 : Durcissement du Cluster

2.1 : Application des Contrôles d'Accès Basés sur les Rôles (RBAC)

2.2 : Gestion Prudente des Comptes de Service

2.3 : Restriction de l'Accès à l'API Kubernetes

2.4 : Mise à Jour Proactive de Kubernetes pour Éviter les Vulnérabilités

Module 3 : Durcissement du Système

3.1 : Réduction de la Surface d'Attaque du Système

3.2 : Principe du Moindre Privilège dans la Gestion des Identités et des Accès

3.3 : Limitation de l'Accès Externe au Réseau

3.4 : Outils de Durcissement du Noyau

Module 4 : Réduction des Vulnérabilités des Microservices

4.1 : Application des Normes de Sécurité des Pods

4.2 : Gestion Sécurisée des Secrets Kubernetes

4.3 : Techniques d'Isolation

4.4 : Mise en œuvre du Chiffrement Pod-à-Pod

Module 5 : Sécurité de la Chaîne d'Approvisionnement

5.1 : Réduction de l'Empreinte des Images de base

5.2 : Sécurisation de la Chaîne d'Approvisionnemt

5.3 : Analyse Statique des Workloads & des Images

5.4 : Signature et Validation des Artefacts

Module 6 : Supervision, Journalisation et Sécurité en Temps Réel

6.1 : Détecter des Activités Malveillantes

6.2 : Détection des Menaces au niveau des Applis, des Infrastructures et des Données

6.3 : Investigation des Attaques et Identification des Acteurs Malveillants

6.4 : Immuabilité des Conteneurs à l'Exécution

6.5 : Exploitation des Logs d'audit Kubernetes