Formation **Certified Kubernetes Security Specialist (préparation à la certification CKS)**

Le programme Certified Kubernetes Security Specialist (CKS) garantit que les titulaires de la certification CKS possèdent les compétences, les connaissances et l'expertise nécessaires pour appliquer un large éventail de bonnes pratiques en matière de sécurisation des applications basées sur des conteneurs et des plateformes Kubernetes, tant lors de la construction que du déploiement et de l'exécution. La certification CKA est requise pour pouvoir passer cet examen. Le coût de l'examen n'est pas inclus dans le tarif de la formation, contactez-nous pour connaître les tarifs en vigueur !

Durée
2 jours

Objectifs pédagogiques

- Se préparer efficacement au passage de l'examen de certification CKS
- Démontrer une expertise dans la sécurisation des applications basées sur des conteneurs et des plateformes Kubernetes
- Mettre en œuvre les meilleures pratiques pour se prémunir contre les menaces à travers l'infrastructure physique, les applications, les réseaux, les données, les utilisateurs et les charges de travail
- Détecter les failles de sécurité potentielles, identifier les phases d'attaque et les acteurs malveillants dans l'environnement, et garantir des mesures de sécurité robustes à chaque étape de l'opération à travers l'ensemble du cycle de développement

Public
Ingénieurs devops, sysadmins, architectes

Prérequis
Être titulaire de la certification CKA, Certified Kubernetes Administrator. Avoir de bonnes connaissances sur les systèmes Unix et les conteneurs, ainsi qu'une expérience de travail significative avec Kubernetes pour l'administration.

Programme de formation

Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

Configuration du cluster

Utiliser les politiques de sécurité du réseau pour restreindre l'accès au niveau du cluster
Utiliser le benchmark CIS pour examiner la configuration de sécurité des composants Kubernetes (etcd, kubelet, kubedns, kubeapi)
Configurer correctement les objets Ingress avec un contrôle de sécurité
Protéger les métadonnées des nœuds et les endpoints
Minimiser l'utilisation et l'accès aux éléments de l'interface graphique
Vérifier les binaries de la plateforme avant de les déployer

Cluster Hardening

Restreindre l'accès à l'API de Kubernetes
Utiliser des contrôles d'accès basés sur les rôles pour minimiser l'exposition
Faire preuve de prudence dans l'utilisation des comptes de service, par exemple en désactivant les valeurs par défaut, en minimisant les autorisations sur les comptes nouvellement créés
Mettre à jour Kubernetes fréquemment

System Hardening

Minimiser l'empreinte du système d'exploitation hôte (réduire la surface d'attaque)
Minimiser les rôles IAM
Minimiser l'accès externe au réseau
Utiliser de manière appropriée les outils de durcissement du noyau tels que AppArmor, seccomp

Minimiser les vulnérabilités des microservices

Configurer des domaines de sécurité appropriés au niveau du système d'exploitation
Gérer les secrets Kubernetes
Utiliser des bacs à sable d'exécution de conteneurs dans les environnements multi-tenants (par exemple, gvisor, conteneurs kata).
Mettre en œuvre le chiffrement de pod à pod par l'utilisation de mTLS

Sécurité de la Supply Chain

Minimiser l'empreinte de l'image de base
Sécurisez votre chaîne d'approvisionnement : établissez une liste blanche des registres autorisés, signez et validez les images.
Utilisez l'analyse statique des charges de travail des utilisateurs (par exemple, ressources Kubernetes, fichiers Docker).
Analyser les images pour détecter les vulnérabilités connues

Surveillance, journalisation et sécurité d'exécution

Effectuer des analyses des processus syscall et des activités de fichiers au niveau de l'hôte et du conteneur pour détecter les activités malveillantes.
Détecter les menaces au sein de l'infrastructure physique, des applications, des réseaux, des données, des utilisateurs et des charges de travail.
Détecter toutes les phases de l'attaque, indépendamment de l'endroit où elle se produit et de la manière dont elle se propage.
Effectuer des recherches analytiques approfondies et identifier les mauvais acteurs au sein de l'environnement.
Garantir l'immuabilité des conteneurs au moment de l'exécution.
Utiliser les journaux d'audit pour surveiller l'accès.

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.