Formation : Kubernetes Security Fundamentals (LFS460)

Cours officiel LFS460, préparation aux examens CKS

Cours pratique - 4j - 28h00 - Réf. GKU
Prix : 3600 € H.T.

Avec cette formation, vous disposerez des connaissances et des compétences nécessaires pour maintenir la sécurité dans des environnements dynamiques et multi-projets. Ce cours aborde les problèmes de sécurité des environnements de production cloud et couvre les sujets liés à la chaîne d'approvisionnement des conteneurs de sécurité, en discutant des sujets antérieurs à la configuration d'un cluster jusqu'au déploiement et à l'utilisation continue, ainsi qu'à l'utilisation agile, y compris où trouver des informations continues sur la sécurité et la vulnérabilité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Savoir maintenir la sécurité dans des environnements dynamiques multi-projets
- Savoir répondre aux problèmes de sécurité des environnements de production cloud
- Se préparer l'examen Certified Kubernetes Security Specialist (CKS)

Public concerné

Toute personne détenant une certification CKA et intéressée ou responsable de la sécurité du cloud.

Prérequis

Posséder la certification "Certified Kubernetes Administration (CKA)".

Certification

Cette formation prépare à la certification "Certified Kubernetes Security Specialist (CKS)".
Comment passer votre examen ?

PARTICIPANTS

Toute personne détenant une certification CKA et intéressée ou responsable de la sécurité du cloud.

PRÉREQUIS

Posséder la certification "Certified Kubernetes Administration (CKA)".

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Méthodes et moyens pédagogiques

Travaux pratiques

La formation comprend des travaux pratiques pour créer et sécuriser un cluster Kubernetes, ainsi que pour surveiller et consigner les événements de sécurité.

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

Programme de la formation

1 Présentation de la sécurité du cloud

- Projets multiples.
- Qu'est-ce que la sécurité ?
- Évaluation, prévention, détection et réaction.
- Classes d'attaquants, types d'attaques et surfaces d'attaque.
- Considérations relatives au matériel et au micrologiciel.
- Agences de sécurité.
- Gérer l'accès externe.

2 Préparation de l'installation

- Chaîne d'approvisionnement d'images.
- Sandbox d'exécution.
- Vérifier les binaires de la plateforme.
- Minimiser l'accès à l'interface graphique.
- Contrôle basé sur des politiques.

3 Installation du cluster

- Mise à jour de Kubernetes.
- Outils pour renforcer le noyau.
- Exemples de renforcement du noyau.
- Atténuation des vulnérabilités du noyau.

4 Sécurisation du serveur Kube-Api

- Restreindre l'accès à l'API.
- Activer l'audit Kube-apiserver.
- Configuration de RBAC.
- Admission de sécurité des pods.
- Minimiser les rôles IAM.
- Protection d'etcd.
- Benchmark CIS.
- Utilisation des comptes de service.

5 Mise en réseau

- Notions de base sur les pare-feu.
- Plugins réseau.
- Atténuer les tentatives de connexion par force brute.
- Objets d'entrée.
- Chiffrement de pod à pod.
- Restreindre l'accès au niveau du cluster.

6 Considérations relatives à la charge de travail

- Minimiser l'image de base.
- Analyse statique des charges de travail.
- Analyse d'exécution des charges de travail.
- Immuabilité des conteneurs.
- Contrôle d'accès obligatoire.
- SELinux.
- AppArmor.
- Générer des profils AppArmor.

7 Détection des problèmes

- Comprendre les phases d'une attaque.
- Préparation.
- Comprendre la progression d'une attaque.
- Gérer un incident.
- Gérer les conséquences d'un incident.
- Systèmes de détection d'intrusion.
- Détection des menaces.
- Analyse comportementale.

8 Avis sur les domaines

- Préparation à l'examen.
- Travaux pratiques.

Dates et lieux

CLASSE À DISTANCE
2026 : 31 mars, 23 juin, 6 oct., 15 déc.

PARIS LA DÉFENSE
2026 : 31 mars, 23 juin, 6 oct., 15 déc.