Publication date : 12/06/2024

Course : Kubernetes Security Fundamentals (LFS460)

Official LFS460 course, CKS exam preparation

Practical course - 4d - 28h00 - Ref. GKU
Price : 3600 € E.T.

With this course, you'll have the knowledge and skills you need to maintain security in dynamic, multi-project environments. This course addresses security issues in cloud production environments and covers topics related to the security container supply chain, discussing topics prior to cluster configuration through to deployment and ongoing use, as well as agile use, including where to find ongoing security and vulnerability information.

Teaching objectives

At the end of the training, the participant will be able to:

- Maintain safety in dynamic, multi-project environments
- Savoir répondre aux problèmes de sécurité des environnements de production cloud
- Preparing for the Certified Kubernetes Security Specialist (CKS) exam

Intended audience

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

Prerequisites

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

Certification

This course prepares you for certification as a "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.

PREREQUISITES

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

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

Practical details

Hands-on work

The course includes practical work on creating and securing a Kubernetes cluster, as well as monitoring and logging security events.

Teaching methods

Training in French. Official course material in digital format and in English. Good understanding of written English.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

Course schedule

1 Cloud security overview

- Multiple projects.
- What is safety?
- Assessment, prevention, detection and response.
- Attacker classes, attack types and attack surfaces.
- Hardware and firmware considerations.
- Security agencies.
- Manage external access.

2 Preparing for installation

- Image supply chain.
- Sandbox execution.
- Check platform binaries.
- Minimize GUI access.
- Policy-based control.

3 Cluster installation

- Kubernetes update.
- Tools to strengthen the core.
- Examples of core reinforcement.
- Mitigate kernel vulnerabilities.

4 Securing the Kube-Api server

- Restrict access to the API.
- Enable Kube-apiserver auditing.
- RBAC configuration.
- Pod safety intake.
- Minimize IAM roles.
- Protection for etcd.
- CIS benchmark.
- Use of service accounts.

5 Networking

- Firewall basics.
- Network plugins.
- Mitigate brute-force connection attempts.
- Input objects.
- Pod-to-pod encryption.
- Restrict access at cluster level.

6 Workload considerations

- Minimize the base image.
- Static analysis of workloads.
- Workload execution analysis.
- Immutability of containers.
- Access control mandatory.
- SELinux.
- AppArmor.
- Generate AppArmor profiles.

7 Problem detection

- Understand the phases of an attack.
- Preparation.
- Understand the progression of an attack.
- Manage an incident.
- Manage the consequences of an incident.
- Intrusion detection systems.
- Threat detection.
- Behavioral analysis.

8 Opinions on domains

- Exam preparation.
- Practical work.

Dates and locations

REMOTE CLASS
2026 : 31 Mar., 23 June, 6 Oct., 15 Dec.

PARIS LA DÉFENSE
2026 : 31 Mar., 23 June, 6 Oct., 15 Dec.