

Warsztat przygotowujący do egzaminu Certified Kubernetes Security Specialist (CKS)

Szkolenie CKS (Certified Kubernetes Security Specialist) jest właśnie dla Ciebie.

Nauczymy Cię stosowania dobrych praktyk bezpiecznej administracji klastrem Kubernetes, pomożemy uzupełnić i zweryfikować wiedzę zdobytą podczas wcześniejszych etapów kształcenia. Przygotujemy Cię do egzaminu certyfikacyjnego, otwierając drogę do zdobycia cenionego na rynku pracy i potwierdzającego specjalistyczne kompetencje certyfikatu



Odbiorcy szkolenia

Zadbaj o bezpieczeństwo w Kubernetesie! Szkolenie CKS (Certified Kubernetes Security Specialist)

- Ukończyłeś szkolenia z Dockera oraz/lub Kubernetesa i chcesz pogłębić swoją wiedzę w tych obszarach?
- Zajmujesz się administracją klastrem Kubernetes i chcesz podnieść poziom jego bezpieczeństwa?
- Posiadasz certyfikat Certified Kubernetes Administrator i myślisz o dalszym rozwoju zawodowym?



Korzyści

Z nami dowiesz się, jak:

- sprawdzać status klastra Kubernetes pod kątem bezpieczeństwa

- uruchamiać aplikacje na klastrze i zarządzać ich konfiguracją
- wykorzystywać benchmarki do zabezpieczania klastra
- bezpiecznie wdrażać i aktualizować klaster
- wdrażać polityki bezpieczeństwa dotyczące różnych aspektów pracy klastra
- audytować i monitorować stan klastra oraz jego elementów
- kontrolować dostęp do klastra

Postaw na wiedzę! Już dziś sprawdź dostępne terminy szkoleń i wybierz odpowiedni.



Program szkolenia

1. Podstawowe informacje o egzaminie:
 - zakres egzaminu CKS
 - przygotowanie przeglądarki pod kątem egzaminu zdalnego
 - sposoby na pracę z oficjalną dokumentacją (wyszukaj, skopiuj, dostosuj)
2. Ogólne spojrzenie na kwestie zabezpieczania klastrów
 - Obiekty Pod, ReplicaSet, Deployment itp.
 - Namespaces a dostępność obiektów przez DNS
 - CIS Benchmarks, NIST Cybersecurity Framework
 - wdrażanie obiektów za pomocą metody deklaratywnej a imperatywnej (opcja dry-run pod kątem egzaminu)
3. Instalacja klastra Kubernetes pod kątem security
 - przygotowanie nodów klastra
 - instalacja uwzględniająca dobre praktyki
4. Zabezpieczanie kube-apiserver
 - zarządzanie i przegląd logów, Audit Log
 - Role Based Access Control
 - Pod Security Policies
 - Service Accounts
 - elementy troubleshootingu
5. Zagadnienia związane z siecią w Kubernetesie:
 - wdrożenie Network Security Policy
 - separacja Podów
 - konfiguracja Ingress Controllera
 - mTLS – zasada działania i wdrożenie, Linkerd
 - testowanie dostępności serwisów kubernetesowych
6. Bezpieczeństwo obrazów i kontenerów wykorzystywanych na klastrze
 - skanowanie obrazów za pomocą Clair, Trivy
 - sposoby na monitorowanie procesów: Auditd, Systemd-Journald, Falco
 - profilowanie aplikacji za pomocą AppArmor, polityki SELinux

- wdrażanie HIDS, NIDS, IDS (projekty Suricata, OSSEC)
7. Zadanie imitujące egzamin certyfikacyjny wraz z omówieniem



Oczekiwane przygotowanie uczestnika

Uczestnictwo w szkoleniach lub adekwatna wiedza na poziomie:

- [ELA010 – Enterprise Linux Administration](#)
- [LX-D – Docker w praktyce](#)
- [LX-K – Kubernetes w praktyce](#)



Szkolenie obejmuje

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty



Język

- Szkolenie: polski
- Materiały: polski

Czas trwania

2 dni / 14 godzin

Opis egzaminu

egzamin CKS