CERTIFIED KUBERNETES SECURITY SPECIALIST (CKS)

Kategoria	Czas trwania	Termin	Cena
DevOps	28h / 4 dni	ustalamy indywidualnie	ustalamy indywidualnie

Program szkolenia:

Poniżej przedstawiamy przykładowy program szkolenia, który może zostać zmodyfikowany zgodnie z oczekiwaniami oraz poziomem grupy szkoleniowej. Przed przygotowaniem docelowego programu szkolenia, przeprowadzamy rozmowę techniczną, w której bierze udział trener oraz osoba techniczna lub cały zespół developerów reprezentujący klienta, w celu ustalenia szczegółów szkolenia.

1. Konfiguracja klastra

- Wykorzystanie zasad bezpieczeństwa sieciowego do ograniczenia dostępu na poziomie klastra
- Wykorzystanie standardu CIS do przeglądu konfiguracji zabezpieczeń komponentów Kubernetes (etcd, kubelet, kubedns, kubeapi)
- Prawidłowe skonfigurowanie obiektów Ingress z kontrolą bezpieczeństwa
- Ochrona metadanych i punktów końcowych węzła
- Minimalizacja korzystania z elementów interfejsu graficznego i dostępu do nich
- Weryfikacja binarnych plików platformy przed wdrożeniem

2. Zabezpieczenie klastra

- Ograniczenie dostępu do interfejsu API Kubernetes
- Wykorzystanie kontroli dostępu opartej na rolach w celu minimalizacji ekspozycji
- Ostrzeżenie przed używaniem kont usługowych, np. wyłączanie domyślnych ustawień i minimalizacja uprawnień dla nowo utworzonych kont
- Regularna aktualizacja Kubernetes

3. Zabezpieczenie systemu

- Minimalizacja śladu systemu operacyjnego hosta (redukcja powierzchni ataku)
- Minimalizacja ról IAM
- Minimalizacja dostępu zewnętrznego do sieci
- Odpowiednie wykorzystanie narzędzi do zabezpieczania jądra, takich jak AppArmor, seccomp

4. Minimalizowanie podatności mikrousług

- Ustawienie odpowiednich dziedzin zabezpieczeń na poziomie systemu operacyjnego
- Zarządzanie tajnymi informacjami Kubernetes
- Wykorzystanie piaskownic środowiska uruchomieniowego kontenerów w środowiskach wielomandantowych (np. gvisor, kata containers)

5. Bezpieczeństwo łańcucha dostaw

- Minimalizacja rozmiaru podstawowego obrazu
- Zabezpieczenie łańcucha dostaw: wykazywanie dozwolonych rejestrów, podpisywanie i walidacja obrazów
- Wykorzystanie statycznej analizy zasobów użytkownika (np. zasoby Kubernetes, pliki Docker)
- Skanowanie obrazów pod kątem znanych podatności

6. Monitorowanie, logowanie i bezpieczeństwo w czasie rzeczywistym

- Wykonywanie analizy zachowań syscall, procesów i aktywności plików na poziomie hosta i kontenera w celu wykrywania działań złośliwych
- Wykrywanie zagrożeń w infrastrukturze fizycznej, aplikacjach, sieciach, danych, użytkownikach i obciążeniach
- Wykrywanie wszystkich faz ataku, niezależnie od tego, gdzie się zaczyna i jak się rozprzestrzenia
- Przeprowadzanie głębokiego analitycznego śledztwa i identyfikacja sprawców w środowisku
- Zapewnienie niemutowalności kontenerów w czasie rzeczywistym
- Wykorzystanie dzienników audytu do monitorowania dostępu