Możliwość dofinansowania

Kurs Kubernetes Security – hardening klastra i ochrona aplikacji ponad ustawienia domyślne

Numer usługi 2026/01/29/52766/3294479

3 013,50 PLN brutto
2 450,00 PLN netto
167,42 PLN brutto/h
136,11 PLN netto/h

NOBLEPROG POLSKA Spółka z o.o

4,4 / 5
923 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
18 h
05.03.2026 do 06.03.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	**Dla kogo jest to szkolenie** • Inżynierowie DevOps / SRE oraz administratorzy platform, którzy utrzymują klastry Kubernetes i odpowiadają za bezpieczeństwo. • Architekci i inżynierowie infrastruktury (on-prem / cloud), którzy projektują standardy i wzorce wdrożeniowe dla zespołów. • Specjaliści bezpieczeństwa i audytorzy techniczni, którzy chcą zrozumieć praktykę zabezpieczania Kubernetesa. • Liderzy techniczni i osoby wdrażające polityki zgodności (np. wymogi korporacyjne, audyty, standardy wewnętrzne). **Wymagania wstępne** • Podstawowa znajomość Kubernetesa: pody, deploymenty, usługi, namespace, kubectl (poziom wprowadzający). • Podstawy Linux i sieci (TCP/IP, porty, DNS, firewall) – na poziomie ogólnym. • Środowisko labowe: komputer z dostępem do internetu oraz narzędzia zgodnie z instrukcją trenera (np. kubectl, klient do klastra, repozytorium ćwiczeń).
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	26-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	18

Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Uczestnik Kurs Kubernetes Security – hardening klastra i ochrona aplikacji ponad ustawienia domyślne zdobędzie wiedzę i umiejętności w zakresie zabezpieczania klastrów Kubernetes, identyfikowania zagrożeń oraz wdrażania praktyk ochrony zasobów i zarządzania dostępem w środowiskach kontenerowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje kluczowe zagrożenia związane z bezpieczeństwem klastra Kubernetes	Uczestnik potrafi wymienić i opisać co najmniej trzy typowe zagrożenia oraz wskazać potencjalne skutki ich wystąpienia.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje proces uwierzytelniania i autoryzacji w Kubernetes, uwzględniając komponenty takie jak certyfikaty, tokeny i RBAC.	Uczestnik analizuje przykładową konfigurację i identyfikuje potencjalne luki w zabezpieczeniach.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje środowisko Kubernetes zgodnie z zasadami hardeningu i zasadą najmniejszych uprawnień.	Uczestnik dokonuje konfiguracji klastra z ograniczoną powierzchnią ataku oraz zabezpieczonym dostępem do API.	Test teoretyczny z wynikiem generowanym automatycznie
Wdraża polityki bezpieczeństwa ograniczające uprawnienia użytkowników, dostęp do sieci i zasobów chmurowych.	Uczestnik tworzy reguły polityk i przypisuje je do odpowiednich ról w scenariuszu warsztatowym.	Test teoretyczny z wynikiem generowanym automatycznie
Ocenia bezpieczeństwo komponentów zewnętrznych (np. dodatków i agentów) oraz przygotowuje plan zarządzania ryzykiem.	Uczestnik identyfikuje zagrożenia związane z użyciem komponentów trzecich i przedstawia plan ich kontroli w projekcie końcowym.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Zakres tematyczny usługi:

Program szkolenia (ramowy – bez zmian)

Wprowadzenie

- Cele szkolenia i zasady pracy warsztatowej.
- Model zagrożeń dla klastra: aktorzy, wektory ataku, typowe błędy operacyjne.

Przegląd API Kubernetesa i funkcji zabezpieczających

- Dostęp do końcówek HTTPS, API Kubernetes, węzłów i kontenerów – gdzie najczęściej powstają „dziury”.
- Uwierzytelnianie i autoryzacja: certyfikaty, tokeny, RBAC – rola control plane i komponentów.

Jak hakerzy atakują Twój klaster

- Jak atakujący lokalizują etcd, API i usługi zarządzające – ekspozycja portów, błędy sieciowe i chmura.
- Uruchamianie kodu w kontenerach i węzłach – typowe scenariusze i sygnały ostrzegawcze.
- Eskalacja uprawnień – od „pod-a” do przejęcia klastra.
- Studium przypadku: incydent z wykorzystaniem klastra Kubernetesa (perspektywa ryzyk i wniosków).

Konfigurowanie Kubernetesa

- Wybór dystrybucji – konsekwencje bezpieczeństwa i wsparcia.
- Instalacja Kubernetesa z myślą o hardeningu: ograniczanie powierzchni ataku od pierwszego dnia.

Używanie poświadczeń i sekretów

- Cykl życia poświadczeń: tworzenie, dystrybucja, rotacja, odwołanie, audyt.
- Sekrety: modele przechowywania, ryzyka, ochrona w etcd.
- Bezpieczna dystrybucja poświadczeń do workloadów – zasada najmniejszych uprawnień.

Kontrolowanie dostępu do API Kubernetesa

- TLS dla ruchu API – poprawna konfiguracja i typowe błędy.
- Uwierzytelnianie: strategie dla użytkowników, usług i automatyzacji.
- Autoryzacja: projektowanie ról i uprawnień, separacja obowiązków, kontrola dostępu administracyjnego.

Kontrolowanie możliwości użytkowników i obciążeń

- Zasady i polityki Kubernetesa – jak przekuć je w praktyczne standardy.
- Ograniczanie zużycia zasobów (requests/limits, quota) – ochrona przed nadużyciem i przypadkowymi awariami.
- Ograniczanie uprawnień kontenerów – minimalne uprawnienia, kontekst bezpieczeństwa, typowe antywzorce.
- Ograniczanie dostępu do sieci – segmentacja i izolacja komunikacji między usługami.

Kontrolowanie dostępu do węzłów

- Rozdzielanie dostępu do obciążeń i administracji – ograniczanie blast radius.
- Praktyki ograniczania dostępu do hosta (node) i rozważania operacyjne.

Ochrona składników klastra

- Ograniczanie dostępu do etcd – kluczowe ryzyko i konsekwencje wycieku.
- Wyłączanie zbędnych funkcji i minimalizacja komponentów.
- Zmiana, usuwanie i odwołanie poświadczeń i tokenów – operacyjny plan reakcji.

Zabezpieczanie obrazu kontenera

- Zarządzanie obrazami Docker i Kubernetesa: źródła, podpisy, kontrola wersji, polityki użycia.
- Budowanie bezpiecznych obrazów: minimalne bazowe obrazy, zasady uruchomieniowe, redukcja podatności.

Kontrolowanie dostępu do zasobów w chmurze

- Metadane platformy chmurowej – dlaczego bywają furtką do eskalacji.
- Ograniczanie uprawnień do zasobów w chmurze – role, service accounts, minimalizacja scope'u.

Ocenianie integracji z trzecimi stronami

- Minimalizacja uprawnień przyznawanych oprogramowaniu trzecich stron (add-ony, operatory, agenty).
- Ocena komponentów, które mogą tworzyć pody – ryzyka łańcucha dostaw i uprawnień.

Ustanawianie polityki zabezpieczeń

- Analiza istniejącego profilu zabezpieczeń – co już działa, a co jest ryzykowne.
- Budowa modelu zabezpieczeń: standardy, odpowiedzialności, wyjątki, proces zmian.
- Zagadnienia bezpieczeństwa natywnego w chmurze – praktyki i pułapki.
- Inne najlepsze praktyki: checklisty wdrożeniowe, standardy obrazów, zasady dostępu i segmentacji.

Szyfrowanie nieużywanych danych

- Szyfrowanie kopii zapasowych – minimalny standard i kontrola dostępu.
- Szyfrowanie całego dysku – kiedy jest wymagane i jak wpływa na operacje.
- Szyfrowanie sekretów w etcd – konfiguracja i konsekwencje.

Monitorowanie aktywności

- Rejestrowanie audit: co logować, jak ograniczyć szum, jak chronić logi.
- Audyt i zarządzanie łańcuchem dostaw oprogramowania – widoczność zmian i zależności.
- Alerty i aktualizacje bezpieczeństwa: subskrypcje, procedury, okna serwisowe.

Podsumowanie i wnioski

- Kluczowe ryzyka i działania o największym wpływie na bezpieczeństwo.
- Plan wdrożenia: quick wins, priorytety, harmonogram oraz odpowiedzialności w zespole.

Walidacja - test teoretyczny z wynikiem generowanym automatycznie.

Wymagania:

- Podstawowa znajomość Kubernetesa: pody, deploymenty, usługi, namespace, kubectl (poziom wprowadzający).
- Podstawy Linux i sieci (TCP/IP, porty, DNS, firewall) – na poziomie ogólnym.
- Środowisko labowe: komputer z dostępem do internetu oraz narzędzia zgodnie z instrukcją trenera (np. kubectl, klient do klastra, repozytorium ćwiczeń).

Informacje o realizacji usługi:

Program obejmuje zarówno aspekty teoretyczne, jak i praktyczne, oparte na ćwiczeniach i przykładach wdrożeniowych. Uczestnik nabywa kompetencje cyfrowe.

Usługa jest realizowana zdalnie w czasie rzeczywistym, co oznacza, że każdy uczestnik w trakcie zajęć pracuje indywidualnie na swoim komputerze.

Metody pracy:

- Interaktywna prezentacja i dyskusja – skupienie na „dlaczego" oraz konsekwencjach decyzji konfiguracyjnych.
- Ćwiczenia praktyczne w laboratorium – krok po kroku z instruktorem, na gotowych scenariuszach ataku i obrony.
- Checklisty i wzorce wdrożeniowe – materiały do wykorzystania po szkoleniu w środowisku produkcyjnym.

Przed szkoleniem uczestnicy będą musieli wypełnić pre-test.

Szkolenie trwa 18 godzin dydaktycznych z czego 10 godzin jest teoretycznych i 8 godzin praktycznych. W trakcie szkolenia przewiduje się przerwy dostosowane do potrzeb uczestników. Przerwy są wliczone w czas trwania szkolenia.

Program kończy się walidacją w formie testu teoretycznego, który weryfikuje osiągnięcie wszystkich efektów uczenia się. Walidacja obejmuje całość procesu, aż do momentu uzyskania oceny efektów uczenia się.

Proces walidacji - test ma na celu ocenę wiedzy i umiejętności uczestników, uwzględniając pytania zamknięte i otwarte. Uczestnicy po ocenie testu zostaną poinformowani o wynikach testu. Usługodawca zapewnia rozdzielność funkcji pomiędzy trenerem a osobą odpowiedzialną za walidację efektów uczenia się.

Minimalny poziom kwalifikowalności poprawnych odpowiedzi w teście wiedzy wynosi 80%.

Po ukończeniu szkolenia wystawiane jest zaświadczenie potwierdzające ukończenie szkolenia i osiągnięcie efektów kształcenia.

Szczegółowe warunki organizacyjne szkolenia:

Usługa jest realizowana zdalnie w czasie rzeczywistym, co oznacza, że każdy uczestnik w trakcie zajęć pracuje indywidualnie na swoim komputerze. Szkolenie będzie składało się z części teoretycznej i praktycznej. Szkolenie realizowane jest zdalnie. Uczestnicy pracują na środowisku laboratoryjnym i realizują zadania praktyczne pod nadzorem trenera.

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo. Usługa rozwojowa nie jest świadczona przez podmiot będący jednocześnie podmiotem korzystającym z usług rozwojowych o zbliżonej tematyce w ramach danego projektu. Usługa rozwojowa nie obejmuje wzajemnego świadczenia usług w projekcie o zbliżonej tematyce przez Dostawców usług, którzy delegują na usługi siebie oraz swoich pracowników i korzystają z dofinansowani a, a następnie świadczą usługi w zakresie tej samej tematyki dla Przedsiębiorcy, który wcześniej występował w roli Dostawcy tych usług. Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności kosztów środków trwałych przekazywanych Przedsiębiorcom lub Pracownikom przedsiębiorcy, kosztów dojazdu i zakwaterowania.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 013,50 PLN
Koszt przypadający na 1 uczestnika netto	2 450,00 PLN
Koszt osobogodziny brutto	167,42 PLN
Koszt osobogodziny netto	136,11 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Kamil Baran

Wykształcenie wyższe.
Doświadczony trener, szkoleniowiec NobleProg; specjalizujący się w Dockerze, orchestracji kontenerów (Kubernetes, Docker Swarm) oraz bazach danych (MongoDB, Microsoft SQL).
Od 2002 roku pracuje jako trener i konsultant dla wiodących firm na polskim i europejskim rynku, a także dla tych nieco mniejszych.
Przeprowadził ponad 150 godzin szkoleniowych z zakresu szkolenia w ciągu ostatnich dwóch latach.
Kurs Pedgogiczny dla wykładowców pozaszkolnych form kształcenia „Europejski wykładowca” 20 sierpnia 2011 r.

Kwalifikacje zdobyte w ostatnich 5 latach

2023-08-28 to 2023-08-31 - Docker and Kubernetes advanced - NobleProg
2023-07-17 to 2023-07-24- Docker and Kubernetes Bespoke - NobleProg
2023-05-15 to 2023-05-18 - Docker and Kubernetes Bespoke - NobleProg
2022.01.26 - Certified Kubernetes Security Specialist
2020.03.18 - Certified Kubernetes Application Developer
2020.02.07 - Certified Kubernetes Administrator
2015.07.21 - M202: MongoDB Advanced Deployment and Operations
2015.07.15 - M102: MongoDB for DBAs
2015.06. - The MongoDB Certified Developer Associate Level
2015.05.06 - M101JS: MongoDB for Node.js Developers

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- Uczestnicy otrzymają dostęp do materiałów online: prezentacja, instrukcje laboratoryjne, repozytorium z przykładami.

Warunki uczestnictwa

- Podstawowa znajomość Kubernetesa: pody, deploymenty, usługi, namespace, kubectl (poziom wprowadzający).
- Podstawy Linux i sieci (TCP/IP, porty, DNS, firewall) – na poziomie ogólnym.
- Środowisko labowe: komputer z dostępem do internetu oraz narzędzia zgodnie z instrukcją trenera (np. kubectl, klient do klastra, repozytorium ćwiczeń).
- Przed szkoleniem uczestnicy będą musieli wypełnić pre-test.
- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% -100 % (w zależności od programu dofinansowania i podpisanej umowy z Operatorem) zajęć usługi rozwojowej.
- Aby uzyskać certyfikat, uczestnik musi być na min 80% zajęć.
- Niespełnienie powyższych wymagań może skutkować brakiem dofinansowania.
- *Harmonogram godzinowy szkolenia każdorazowo dostosowywany jest do grupy szkoleniowej.*
- *Godziny realizacji poszczególnych modułów szkolenia mogą ulec zmianie.*
- *W razie potrzeby szkolenie zostanie dostosowane do osób z niepełnosprawnością.*

Informacje dodatkowe

Informacje dodatkowe

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Koordynacja szkolenia

W sprawie organizacji szkolenia prosimy o kontakt z Patrycją Dobrzyńską: patrycja.dobrzynska@nobleprog.com 880 997 760.

W sprawie dofinansowania do szkolenia prosimy o kontakt z Martą Święcicką: marta.swiecicka@nobleprog.com, 883 407 700

Warunki techniczne

Do realizacji szkoleń online korzystamy z platformy Zoom lub MS Teams oraz DaDesktop. Każdy uczestnik otrzymuje 2 dni przed szkoleniem link do platformy internetowej (na wskazany adres mailowy), na której znajdować się będzie transmisja online. Uczestnictwo w streamingu nie wymaga żadnych, specjalnych oprogramowań: wystarczy, że komputer jest podłączony do Internetu (należy korzystać z przeglądarek: Google Chrome, Mozilla Firefox lub Safari). Uczestnicy oglądają i słuchają na żywo tego, co dzieje się w sali szkoleniowej oraz śledzą treści wyświetlane na komputerze prowadzącego. Dodatkowo, wszyscy mogą zadawać pytania za pośrednictwem chatu online. W przypadku mniejszych szkoleń uczestnicy mogą przez mikrofon komunikować się z trenerem i innymi uczestnikami kursu. Do szkolenia potrzebna jest kamera. Rekomendowany drugi monitor dla komfortu pracy.

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: Dwurdzeniowy procesor Intel Core i5 2,5 GHz i wyższy.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: pobieranie: 10 Mb/s, wysyłanie: 5 Mb/s.

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Nie trzeba pobierać oprogramowania. Aby wziąć udział w szkoleniu online potrzebny jest komputer, laptop, telefon lub tablet ze stabilnym internetem i bez blokad firmowych.

Podczas szkoleń online wykorzystujemy następujące funkcjonalności:

1) Praca w grupach (breakout rooms)

- trener może podzielić uczestników automatycznie lub manualnie

- trener ustala czas trwania pracy w grupach

- pojawia się krótki komunikat na ekranie uczestnika, który informuje, że gospodarz zaprasza do pokoju

- prowadzący może wysłać wiadomość do wszystkich pokoi jednocześnie, np. z opisem zadania do wykonania.

2) Narzędzia dostępne podczas sesji w breakout rooms:

- tablica, możliwość pisania mają wszyscy uczestnicy, efekt pracy można zapisać i pokazać w pokoju szkoleniowym, wszystkim uczestnikom szkolenia

- pokazywanie ekranu, każdy uczestnik może udostępnić swój ekran

- czat

- użytkownik pracujący w pokoju, może w dowolnym momencie zaprosić prowadzącego do pokoju grupowego.

Kontakt

Bartosz Wójcik

E-mail bartosz.wojcik@nobleprog.com

Telefon (+48) 696 100 010