Możliwość dofinansowania

Cyberbezpieczeństwo dla specjalistów IT w JST i przedsiębiorstwach- szkolenie praktyczne

Numer usługi 2025/11/17/164038/3152577

750,00 PLN brutto
750,00 PLN netto
93,75 PLN brutto/h
93,75 PLN netto/h

LIFEPASS spółka z ograniczoną odpowiedzialnością

4,7 / 5

530 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
8 h
06.02.2026 do 06.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie jest skierowane do specjalistów IT odpowiedzialnych za utrzymanie i bezpieczeństwo infrastruktury teleinformatycznej w jednostkach samorządu terytorialnego oraz w przedsiębiorstwach. Uczestnikami mogą być administratorzy systemów i sieci, pracownicy działów bezpieczeństwa IT, specjaliści helpdesk z doświadczeniem technicznym oraz osoby wspierające procesy związane z ochroną systemów i usług. Grupa obejmuje osoby z podstawową lub średnio zaawansowaną wiedzą z zakresu sieci komputerowych, usług serwerowych, bezpieczeństwa poczty i serwisów WWW. Szkolenie przeznaczone jest dla pracowników realizujących zadania związane z monitorowaniem zagrożeń, analizą incydentów, wdrażaniem mechanizmów ochronnych oraz utrzymaniem ciągłości działania środowisk IT.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	05-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Uczestnik po zakończeniu szkolenia będzie rozpoznawał zagrożenia cyberbezpieczeństwa, stosował zasady ochrony informacji oraz bezpiecznej pracy z danymi, tworzył i wykorzystywał silne hasła oraz uwierzytelnianie 2FA, analizował i oceniał ryzykowne sytuacje, a także reagował na incydenty bezpieczeństwa i zgłaszał je zgodnie z procedurami obowiązującymi w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik charakteryzuje podstawowe zagrożenia cyberbezpieczeństwa oraz mechanizmy ich wykrywania.	Uczestnik klasyfikuje typy ataków (np. MITM, DDoS, malware) na podstawie opisu przypadku.	Test teoretyczny
	Uczestnik opisuje działanie podstawowych narzędzi i logów wykorzystywanych do wykrywania incydentów.	Test teoretyczny
Uczestnik opisuje zasady projektowania bezpiecznej infrastruktury sieciowej i usług WWW	Uczestnik wyjaśnia zastosowanie segmentacji sieci, DMZ i kontroli dostępu.	Test teoretyczny
	Uczestnik określa rolę SPF, DKIM, DMARC oraz zabezpieczeń SSL/TLS w ochronie systemów.	Test teoretyczny
Uczestnik analizuje incydenty bezpieczeństwa i dobiera odpowiednie działania reagowania.	Uczestnik identyfikuje rodzaj ataku na podstawie przedstawionych logów lub sytuacji.	Obserwacja w warunkach symulowanych
	Uczestnik formułuje działania naprawcze i eskalacyjne zgodnie z procedurami CSIRT/CERT.	Obserwacja w warunkach symulowanych
Uczestnik projektuje podstawowe środki ochrony infrastruktury IT, poczty i serwisów WWW	Uczestnik dobiera właściwe mechanizmy zabezpieczeń (WAF, konfiguracja DNS, polityki dostępu) do scenariusza.	Obserwacja w warunkach symulowanych
	Uczestnik przygotowuje schemat polityki backupu zgodny z zasadą 3-2-1 i uwzględnia testowanie odtwarzania.	Obserwacja w warunkach symulowanych
Uczestnik współorganizuje proces reagowania na incydenty, stosując zasady komunikacji technicznej i raportowania.	Uczestnik przygotowuje jasny i uporządkowany raport incydentu zawierający wymagane elementy.	Obserwacja w warunkach symulowanych

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

Tytuł: Cyberbezpieczeństwo dla specjalistów IT w JST i przedsiębiorstwach- szkolenie praktyczne

Forma świadczenia usługi: zdalna w czasie rzeczywistym

Czas trwania usługi: 8 godzin dydaktycznych

Godziny realizacji: 8:30 do 14:30

Teoria: 4 godziny dydaktyczne

Praktyka: 3 godziny dydaktyczne

Przerwy: 1 godzina dydaktyczna wliczona w czas szkolenia

Cele szkolenia:

Uczestnik po zakończeniu szkolenia będzie rozpoznawał zagrożenia cyberbezpieczeństwa, stosował zasady ochrony informacji oraz bezpiecznej pracy z danymi, tworzył i wykorzystywał silne hasła oraz uwierzytelnianie 2FA, analizował i oceniał ryzykowne sytuacje, a także reagował na incydenty bezpieczeństwa i zgłaszał je zgodnie z procedurami obowiązującymi w organizacji.

Grupa docelowa:

Szkolenie jest skierowane do specjalistów IT odpowiedzialnych za utrzymanie i bezpieczeństwo infrastruktury teleinformatycznej w jednostkach samorządu terytorialnego oraz w przedsiębiorstwach. Uczestnikami mogą być administratorzy systemów i sieci, pracownicy działów bezpieczeństwa IT, specjaliści helpdesk z doświadczeniem technicznym oraz osoby wspierające procesy związane z ochroną systemów i usług. Grupa obejmuje osoby z podstawową lub średnio zaawansowaną wiedzą z zakresu sieci komputerowych, usług serwerowych, bezpieczeństwa poczty i serwisów WWW. Szkolenie przeznaczone jest dla pracowników realizujących zadania związane z monitorowaniem zagrożeń, analizą incydentów, wdrażaniem mechanizmów ochronnych oraz utrzymaniem ciągłości działania środowisk IT.

Liczba osób: max 20 uczestników

Terener i walidator:

W ramach realizacji usługi zachowany jest wyraźny podział ról trenera i walidatora, zgodnie z wymaganiami systemu BUR.

Trener odpowiada za przygotowanie i przeprowadzenie procesu edukacyjnego, w tym za wsparcie uczestników w osiąganiu założonych efektów uczenia się oraz za zebranie wymaganych dowodów i deklaracji uczestników.

Walidator nie uczestniczy w procesie szkoleniowym i nie wpływa na sposób przygotowania dokumentacji. Jego zadaniem jest niezależna ocena efektów uczenia się osiągniętych przez uczestników, na podstawie przekazanych materiałów. Ocena ta odbywa się zgodnie z przyjętymi standardami walidacji, przy zachowaniu pełnej neutralności i obiektywizmu.

Zakres tematyczny szkolenia:

Wprowadzenie do cyberbezpieczeństwa w organizacji

• Cele szkolenia, kluczowe pojęcia, rola specjalistów IT w ochronie środowiska organizacji.

Podstawy bezpieczeństwa sieci

• Segmentacja sieci, VLAN, zapory, DMZ, kontrola dostępu.

• Monitorowanie ruchu i wykrywanie anomalii.

• Analiza przykładów poprawnej i błędnej architektury.

Najpopularniejsze ataki i metody reagowania

• Ataki MITM, malware, DDoS, brute force.

• Analiza logów i identyfikacja ataków.

• Mechanizmy wykrywania i przeciwdziałania.

Zabezpieczanie poczty elektronicznej i serwisów WWW

• SPF, DKIM, DMARC, ochrona przed spoofingiem.

• SSL/TLS, aktualizacje CMS, bezpieczeństwo formularzy.

• WAF i ochrona aplikacji webowych.

Ochrona przed atakami DDoS i zarządzanie kopiami zapasowymi

• Mechanizmy obronne, limitacja ruchu, load balancing.

• Przepływ ruchu i analiza zachowań botnetów.

• Zasada backupów 3-2-1, backup offline, testy odtwarzania.

Źródła wiedzy o zagrożeniach i reagowanie na incydenty

• CSIRT NASK, CERT, portale branżowe, bazy podatności.

• Procedury zgłaszania, eskalacji i dokumentowania incydentów.

• Komunikacja techniczna i raportowanie.

Podstawy zapewnienia ciągłości działania

• Analiza ryzyka IT i identyfikacja zasobów krytycznych.

• Plan utrzymania dostępności usług.

• Testowanie planów awaryjnych i omówienie praktycznych wyzwań.

Walidacja usługi

Metody szkoleniowe:

- Wykłady teoretyczne.
- Prezentacja
- Ćwiczenia praktyczne
- Konsultacje indywidualne i grupowe
- Dyskusje grupowe: Rozwiązywanie problemów i analiza przypadków.

Weryfikacja efektów uczenia się:

- Test wiedzy (pre- i post-test)
- Feedback od prowadzącego
- Test walidacyjny
- Ankieta ewaluacyjna

Harmonogram

Liczba przedmiotów/zajęć: 11

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Powitanie uczestników oraz przedstawienie trenera celów szkolenia zasad pracy i zakresu tematycznego.	Stanisław Chyb	06-02-2026	08:30	08:45	00:15
2 z 11 Podstawy bezpieczeństwa sieci Omówienie segmentacji sieci zapór DMZ kontroli dostępu oraz analiza przykładów poprawnej i błędnej architektury.	Stanisław Chyb	06-02-2026	08:45	09:30	00:45
3 z 11 Ataki i metody reagowania Przedstawienie popularnych ataków oraz sposobów wykrywania i reagowania z wykorzystaniem analizy logów.	Stanisław Chyb	06-02-2026	09:30	10:15	00:45
4 z 11 Przerwa	Stanisław Chyb	06-02-2026	10:15	10:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 11 Zabezpieczenie poczty i serwisów WWW Omówienie SPF DKIM DMARC oraz ochrony serwisów WWW z użyciem SSL TLS aktualizacji CMS i zabezpieczeń aplikacyjnych.	Stanisław Chyb	06-02-2026	10:30	11:15	00:45
6 z 11 Ochrona przed DDoS i kopie zapasowe Przedstawienie metod obrony przed DDoS oraz planowania i testowania kopii zapasowych zgodnie z zasadą 3-2-1.	Stanisław Chyb	06-02-2026	11:15	12:00	00:45
7 z 11 Przerwa	Stanisław Chyb	06-02-2026	12:00	12:15	00:15
8 z 11 Źródła wiedzy i incydenty Zaprezentowanie roli CSIRT CERT oraz zasad zgłaszania incydentów ich dokumentowania i eskalacji w organizacji.	Stanisław Chyb	06-02-2026	12:15	13:00	00:45
9 z 11 Ciągłość działania Omówienie analizy ryzyka zasobów krytycznych i planów awaryjnych wraz z praktycznymi aspektami utrzymania dostępności usług.	Stanisław Chyb	06-02-2026	13:00	13:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 11 Omówienie głównych zagadnień poruszonych podczas szkolenia oraz wyjaśnienie wątpliwości zgłoszonych przez uczestników.	Stanisław Chyb	06-02-2026	13:45	14:15	00:30
11 z 11 Walidacja usługi	Stanisław Chyb	06-02-2026	14:15	14:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	750,00 PLN
Koszt przypadający na 1 uczestnika netto	750,00 PLN
Koszt osobogodziny brutto	93,75 PLN
Koszt osobogodziny netto	93,75 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Stanisław Chyb

Oficer Wojska Polskiego od 2012 r. w czynnej służbie. Absolwent Wojskowej Akademii Technicznej w Warszawie, Uniwersytetu Ekonomicznego we Wrocławiu oraz Wyższej Szkoły Biznesu – National Louis University z siedzibą w Nowym Sączu. Specjalista w zakresie łączności, teleinformatyki, cyberbezpieczeństwa i kryptografii oraz szeroko pojętego zarządzania (ZZL, technologią, procesami i projektami). Instruktor survivalowych kursów przygotowawczych obejmujących elementy S.E.R.E. Podczas 13-letniej praktyki zawodowej zajmował stanowiska kierownicze zarówno w strukturach krajowych, jak i międzynarodowych, skutecznie przekazując wiedzę podwładnym i współpracownikom. Posiada bogate doświadczenie zawodowe potwierdzone wyróżnieniami w

zakresie bezpieczeństwa, organizacji i eksploatacji systemów łączności i informatyki, a także zarządzania projektami i procesami oraz przywództwa. Auditor wiodący Systemów Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzymuje kompletny skrypt szkoleniowy w pdf zawierający najważniejsze informacje i materiały omawiane podczas zajęć.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach i doradztwie, które dofinansowane są z funduszy europejskich jest założenie konta indywidualnego, a później firmowego w Bazie Usług Rozwojowych. Następnie zapis na wybrane szkolenie za pośrednictwem Bazy Usług Rozwojowych, spełnienie warunków przedstawionych przez danego Operatora, który dysponuje funduszami. Złożenie dokumentów o dofinansowanie do usługi rozwojowej u Operatora Usługi, zgodnie z wymogami jakie określił.

Ponadto niezbędnym warunkiem do nabycia kompetencji jest pełnoletność, wykształcenie co najmniej średnie, wypełnienie testu wiedzy lub odbycie rozmowy kwalifikacyjnej przed i po szkoleniu.

Informacje dodatkowe

Planujemy trzy 15 minutowe przerwy pomiędzy modułami. Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%.W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Warunkiem zaliczenia jest napisanie pre i post testów oraz testu walidacyjnego.

Uczestnictwo w min. 80% zajęć liczone na podstawie listy obecności w każdym dniu szkolenia.

Uczestnicy są świadomi, że usługa realizowana z dofinansowaniem może podlegać monitoringowi ze strony Operatora lub PARP i wyrażają zgodę na jego przeprowadzenie.

Uczestnik otrzyma zaświadczenie ze szkolenia.

Warunki techniczne

Warunki techniczne

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, łącze internetowe – min. 5mb/s
- Przeglądarka internetowa – Chrome, Firefox lub Microsoft Edge. W przypadku Mac OS – Safari
- Aby móc korzystać z usługi na niektórych urządzeniach mobilnych, konieczne może być pobranie odpowiedniej aplikacji w iTunes App Store lub Google Play Store. Do korzystania z usługi w pełnym zakresie dźwięku i obrazu podczas konferencji, konieczne jest posiadanie, mikrofonu lub zestawu słuchawkowego, lub głośników podłączonych do urządzenia i rozpoznanych przez Państwa urządzenie i nie powinny być one jednocześnie używane przez żadną inną aplikację.
- Uczestnik musi mieć zapewniony sprzęt komputerowy we własnym zakresie z dostępem do kamery i mikrofonu.

Kontakt

Lucyna Kuchta

E-mail kontakt@edumeo.pl

Telefon (+48) 577 203 338