Możliwość dofinansowania

Cyberbezpieczeństwo w Praktyce: Ochrona Organizacji i Użytkowników

Numer usługi 2025/01/31/164038/2533784

4 000,00 PLN brutto
4 000,00 PLN netto
200,00 PLN brutto/h
200,00 PLN netto/h

LIFEPASS spółka z ograniczoną odpowiedzialnością

★★★★★

Kielce / stacjonarna
Usługa szkoleniowa
20 h
26.06.2025 do 27.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Specjaliści IT, administratorzy sieci i technicy odpowiedzialni za bezpieczeństwo infrastruktury IT. • Menedżerowie IT oraz osoby zarządzające bezpieczeństwem informatycznym w firmach i instytucjach. • Pracownicy działów bezpieczeństwa, compliance oraz audytorzy zajmujący się ochroną danych i zgodnością z przepisami. • Właściciele małych i średnich przedsiębiorstw (SME), odpowiedzialni za bezpieczeństwo firmowych systemów i ochronę danych klientów. • Kadra zarządzająca, dyrektorzy i menedżerowie chcący wdrożyć skuteczne strategie zabezpieczeń oraz reagować na incydenty cybernetyczne. • Osoby prywatne zainteresowane ochroną swojej tożsamości cyfrowej oraz zabezpieczeniem urządzeń mobilnych i komputerów przed zagrożeniami w sieci. • Użytkownicy technologii chcący lepiej zrozumieć i przeciwdziałać cyberatakom, takim jak phishing, ransomware i malware.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	25-06-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	20
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przekazanie uczestnikom praktycznej wiedzy i umiejętności z zakresu cyberbezpieczeństwa, aby mogli skutecznie identyfikować, zapobiegać i reagować na zagrożenia cyfrowe. Uczestnicy nauczą się, jak chronić infrastrukturę IT, zabezpieczać dane, zarządzać incydentami bezpieczeństwa oraz stosować zaawansowane techniki ochrony przed atakami, takimi jak phishing, malware i ransomware. Szkolenie zwiększy świadomość oraz zdolność obrony przed cyberatakami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje główne zagrożenia cybernetyczne (phishing, ransomware, malware).	Uczestnik udziela prawidłowych odpowiedzi na pytania w quizie dotyczącym rodzajów ataków.	Test teoretyczny
Uczestnik wdraża zasady zarządzania hasłami i uwierzytelnianiem dwuskładnikowym (2FA).	Uczestnik wdraża 2FA podczas ćwiczeń praktycznych.	Test teoretyczny
Uczestnik stosuje procedury odpowiedzi na incydenty bezpieczeństwa.	Uczestnik reaguje skutecznie na symulowany atak w ramach ćwiczeń.	Test teoretyczny
Uczestnik zabezpiecza urządzenia mobilne, stosując odpowiednie metody ochrony.	Uczestnik omawia i stosuje zabezpieczenia na urządzeniach mobilnych.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji

Program

Dzień 1: Wprowadzenie do zagrożeń i ochrona przed cyberatakami

1. **Wprowadzenie do cyberbezpieczeństwa i współczesnych zagrożeń**
   - Omówienie kluczowych pojęć związanych z cyberbezpieczeństwem.
   - Aktualne zagrożenia w świecie cyfrowym (m.in. ataki na systemy chmurowe, IoT).
   - Znaczenie ochrony dla organizacji i osób prywatnych.
   - Zagadnienia techniczne: systemy zabezpieczenia obiektu, zasilania, budowa sieci LAN/WAN/WiFi.
2. **Phishing, ransomware, malware – rozpoznawanie i zapobieganie**
   - Omówienie najczęściej spotykanych zagrożeń.
   - Rodzaje phishingu (e-mailowy, smishing, vishing) i techniki socjotechniczne.
   - Przykłady realnych incydentów oraz techniki wykorzystania AI w atakach.
   - Praktyczne wykorzystanie AI do symulacji ataków.
3. **Zarządzanie incydentami bezpieczeństwa – jak reagować na cyberatak**
   - Procedury odpowiedzi na incydenty: identyfikacja, izolacja, ocena skutków, przywrócenie operacyjności.
   - Tworzenie zespołu reagowania (CSIRT) i procedury eskalacji.
   - Zgłaszanie incydentów w kontekście ochrony osób prywatnych.
4. **Bezpieczeństwo sieci i infrastruktury IT – ochrona serwerów i połączeń**
   - Narzędzia ochrony sieci firmowej: firewalle, IDS, IPS, VPN.
   - Monitorowanie ruchu sieciowego i wykrywanie anomalii.
   - Zagadnienia techniczne: skanowanie sieci, działanie programów antywirusowych, pokaz VPN.
5. **Warsztat: Symulacja ataku phishingowego i reakcja**
   - Interaktywna symulacja ataku phishingowego.
   - Rozpoznawanie podejrzanych sygnałów i podejmowanie kroków zabezpieczających.
6. **Zarządzanie hasłami i uwierzytelnianiem – klucz do ochrony tożsamości cyfrowej**
   - Tworzenie i zarządzanie silnymi hasłami.
   - Korzystanie z menedżerów haseł i metod uwierzytelniania dwuskładnikowego (2FA).
   - Technologia MFA oraz pokaz generatorów haseł.

Dzień 2: Zaawansowane aspekty ochrony danych i infrastruktury IT

1. **Bezpieczne korzystanie z urządzeń mobilnych – ochrona smartfonów i tabletów**
   - Zagrożenia związane z urządzeniami mobilnymi w firmie i prywatnie (BYOD).
   - Najlepsze praktyki bezpieczeństwa: szyfrowanie, biometryka, unikanie nieautoryzowanych aplikacji.
2. **Postępowanie z nośnikami danych i tworzenie kopii zapasowych**
   - Bezpieczne przechowywanie i transport nośników danych (pendrive'y, dyski zewnętrzne).
   - Znaczenie tworzenia kopii zapasowych i testowania ich przywracania.
3. **Ochrona logów systemowych i monitorowanie infrastruktury**
   - Zabezpieczanie logów przed manipulacją.
   - Narzędzia monitorowania i analizowania logów w czasie rzeczywistym.
   - Zagadnienia techniczne: analiza logów systemowych.
4. **Przesyłanie informacji – zabezpieczanie danych w podróży**
   - Szyfrowanie wiadomości e-mail i plików.
   - Korzystanie z publicznych sieci Wi-Fi i narzędzi VPN.
5. **Warsztat: Szacowanie ryzyka w obszarze bezpieczeństwa informacji**

- Identyfikacja i ocena ryzyk związanych z cyberbezpieczeństwem.
- Opracowanie planu zarządzania ryzykiem: analiza słabych punktów i propozycje zabezpieczeń.
- Symulacja „oblężonej cyfrowej twierdzy” – uczestnicy wcielają się w role atakujących i obrońców.

6. **Walidacja usługi**

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wprowadzenie do cyberbezpieczeństwa i współczesnych zagrożeń Omówienie kluczowych pojęć i aktualnych zagrożeń (chmura, IoT) Systemy zabezpieczenia obiektu, zasilania, budowa sieci LAN/WAN/WiFi	Katarzyna Brodnicka	26-06-2025	09:00	10:30	01:30
2 z 15 Przerwa	Katarzyna Brodnicka	26-06-2025	10:30	10:40	00:10
3 z 15 Przerwa	Katarzyna Brodnicka	26-06-2025	10:30	10:40	00:10
4 z 15 Phishing, ransomware, malware – rozpoznawanie i zapobieganie Rodzaje phishingu (e-mailowy, smishing, vishing), techniki socjotechniczne Przykłady realnych incydentów i wykorzystania AI w atakach	Katarzyna Brodnicka	26-06-2025	10:40	12:10	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 15 Przerwa	Katarzyna Brodnicka	26-06-2025	12:10	12:40	00:30
6 z 15 Zarządzanie incydentami bezpieczeństwa – jak reagować na cyberatak Procedury identyfikacji, izolacji, oceny skutków i przywracania operacyjności	Katarzyna Brodnicka	26-06-2025	12:40	14:10	01:30
7 z 15 Przerwa	Katarzyna Brodnicka	26-06-2025	14:10	14:20	00:10
8 z 15 Warsztat: Symulacja ataku phishingowego i reakcja Rozpoznawanie podejrzanych sygnałów i podejmowanie kroków zabezpieczających Zarządzanie hasłami i uwierzytelnianiem	Katarzyna Brodnicka	26-06-2025	14:20	16:30	02:10
9 z 15 Bezpieczne korzystanie z urządzeń mobilnych – zagrożenia i ochrona smartfonów, tabletów Szyfrowanie, biometryka, unikanie nieautoryzowanych aplikacji Postępowanie z nośnikami danych	Katarzyna Brodnicka	27-06-2025	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 15 Ochrona logów systemowych i monitorowanie infrastruktury Narzędzia do analizowania logów w czasie rzeczywistym Szyfrowanie wiadomości e-mail i plików, bezpieczne korzystanie z publicznych sieci Wi-Fi	Katarzyna Brodnicka	27-06-2025	10:40	12:10	01:30
11 z 15 Przerwa	Katarzyna Brodnicka	27-06-2025	12:10	12:40	00:30
12 z 15 Warsztat: Szacowanie ryzyka w obszarze bezpieczeństwa informacji Identyfikacja i ocena ryzyk, analiza słabych punktów i zabezpieczeń	Katarzyna Brodnicka	27-06-2025	12:40	14:10	01:30
13 z 15 Przerwa	Katarzyna Brodnicka	27-06-2025	14:10	14:20	00:10
14 z 15 Symulacja „oblężonej cyfrowej twierdzy” – uczestnicy jako atakujący i obrońcy Podsumowanie szkolenia, sesja pytań i odpowiedzi	Katarzyna Brodnicka	27-06-2025	14:20	16:15	01:55
15 z 15 Walidacja usługi	-	27-06-2025	16:15	16:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 000,00 PLN
Koszt przypadający na 1 uczestnika netto	4 000,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Katarzyna Brodnicka

Katarzyna Brodnicka to doświadczona ekspertka w dziedzinie bezpieczeństwa informacji, ochrony danych oraz cyberbezpieczeństwa. Posiada bogate doświadczenie zawodowe, które zdobywała w różnych instytucjach, m.in. jako Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001:2022, a także jako Inspektor Ochrony Danych (IOD). W ramach swojej kariery zawodowej, Katarzyna specjalizuje się w prowadzeniu audytów, zarządzaniu ryzykiem oraz wdrażaniu polityk bezpieczeństwa zarówno w administracji, jak i w sektorze prywatnym. Ponadto zajmuje się opracowywaniem dokumentacji technicznych, wdrażaniem rozwiązań technologicznych i prowadzeniem szkoleń z zakresu cyberbezpieczeństwa zarówno dla kadry zarządzającej, jak i zespołów technicznych. Prowadzi również własną Kancelarię Audytorską "KB Brand," oferując wsparcie w zakresie audytów, szkoleń oraz wdrażania polityk bezpieczeństwa. Jest ceniona za profesjonalizm, szeroką wiedzę oraz umiejętność dostosowywania metod szkoleniowych do specyficznych potrzeb klientów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzymuje zaświadczenie ukończenia szkolenia.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach i doradztwie, które dofinansowane są z funduszy europejskich jest założenie konta 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.

Informacje dodatkowe

Czas trwania usługi szkoleniowej to 20 godzin dydaktycznych (1 godzina dydaktyczna= 45 minut). Szkolenie zaplanowane jest jako dwudniowe, planowane dwie przerwy w każdym dniu po 10 min i jedna 30 minutowa- obiadowa. 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 uczestnictwo w 80% zajęć.

Adres

ul. 1 Maja 191
25-646 Kielce
woj. świętokrzyskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Lucyna Kuchta

E-mail kontakt@edumeo.pl
Telefon (+48) 577 203 338