Możliwość dofinansowania

Cyberbezpieczeństwo w praktyce, czyli jak chronić swoje dane w sieci - szkolenie

Numer usługi 2025/03/26/43841/2650903

2 800,00 PLN brutto
2 800,00 PLN netto
164,71 PLN brutto/h
164,71 PLN netto/h

Spatium Development Group Sp. z o.o.

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
17 h
12.06.2025 do 13.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Przedmiotowa usługa szkoleniowa skierowana jest dla osób dorosłych, które z własnej inicjatywy chcą podnieść swoje kompetencje i umiejętności. Uczestnik nie musi posiadać wiedzy w zakresie niniejszego szkolenia.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	08-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	17
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Usługa "Cyberbezpieczeństwo w praktyce, czyli jak chronić swoje dane w sieci - szkolenie" przygotowuje do samodzielnego identyfikowania i rozumienia źródeł zagrożeń cyberataków oraz podniesienia świadomości w zakresie ochrony danych i bezpieczeństwa cyfrowego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje potencjalne źródła ataków cyfrowych.	- wskazuje różne źródła zagrożeń dla infrastruktury IT i pracowników - opisuje mechanizmy działania ataków typu ransomware i phishing - omawia ryzyka związane z nowymi technologiami (AI, chmura, urządzenia mobilne) - rozróżnia ataki na systemy IT i OT	Test teoretyczny z wynikiem generowanym automatycznie
Wykorzystuje zasady bezpieczeństwa cyfrowego w organizacji.	- wdraża procedury bezpieczeństwa danych - tworzy bezpieczne hasła i wykorzystuje menedżery haseł oraz klucze U2F - korzysta z szyfrowania poczty oraz danych wrażliwych - organizuje bezpieczne przechowywanie i przesyłanie danych	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje i wdraża normy oraz regulacje dotyczące ochrony informacji i danych cyfrowych.	- rozpoznaje podstawowe akty prawne związane z ochroną danych	Test teoretyczny z wynikiem generowanym automatycznie
Reaguje na różnego rodzaju ataki na urządzeniach mobilnych.	- wdraża odpowiednie procedury bezpieczeństwa - odróżnia prawdziwe maile od potencjalnie fałszywych czy phishingowych - śledzi ewentualne zmiany w trendach dotyczących nietypowych maili	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, 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

A. Wymagania i normy ISO/IEC 27001:

1. Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT.
2. Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT.
3. Algorytmy sztucznej inteligencji, chmura, rozwiązania mobilne.
4. Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie.
5. Źródła ataków cyfrowych.
6. Zasada działania ransomware, sposoby ochrony.
7. Szyfrowanie poczty oraz danych wrażliwych, tworzenie szyfrowanych magazynów danych, metody bezpiecznej wymiany danych.
8. Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z tzw. menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F.
9. Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych.
10. LiveHacking czyli pokaz kontrolowanego ataku analizując krok po kroku zachowanie atakującego firmę hackera.
11. Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania.
12. Walidacja usługi - test teoretyczny z wynikiem generowanym automatycznie

Szkolenie adresowane jest osób dorosłych, które z własnej inicjatywy chcą podnieść swoje kompetencje, umiejętności lub kwalifikacji w zakresie niniejszego szkolenia. Szkolenie trwa 17 godzin dydaktycznych. Przerwy wliczają się do czasu trwania usługi. Maksymalna ilość osób w grupie wynosi 20. Od uczestników wymagany jest dostęp do Internetu i sprzętu komputerowego, który odbiera i przekazuje dźwięk. Realizacja zadań i ćwiczeń będzie przeprowadzona w taki sposób, aby stopniowo narastał ich stopień trudności, ale ich realizacja była w zasięgu możliwości uczestników.

Harmonogram

Liczba przedmiotów/zajęć: 13

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 **Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT. Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę - prezentacja na żywo, chat, ćwiczenia**	**Wojciech Bobak**	**12-06-2025**	**08:00**	**10:00**	**02:00**
2 z 13 **Przerwa**	**Wojciech Bobak**	**12-06-2025**	**10:00**	**10:15**	**00:15**

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 13 Algorytmy sztucznej inteligencji, chmura, rozwiązania mobilne - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	12-06-2025	10:15	12:15	02:00
4 z 13 Przerwa	Wojciech Bobak	12-06-2025	12:15	13:00	00:45
5 z 13 Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie. Źródła ataków cyfrowych. Zasada działania ransomware, sposoby ochrony - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	12-06-2025	13:00	14:45	01:45
6 z 13 Szyfrowanie poczty oraz danych wrażliwych, tworzenie szyfrowanych magazynów danych, metody bezpiecznej wymiany danych - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	13-06-2025	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 13 Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z tzw. menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F.- prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	13-06-2025	09:00	10:00	01:00
8 z 13 Przerwa	Wojciech Bobak	13-06-2025	10:00	10:15	00:15
9 z 13 Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	13-06-2025	10:15	11:15	01:00
10 z 13 LiveHacking czyli pokaz kontrolowanego ataku analizując krok po kroku zachowanie atakującego firmę hackera - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	13-06-2025	11:15	12:15	01:00
11 z 13 Przerwa	Wojciech Bobak	13-06-2025	12:00	12:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 13 Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania - prezentacja na żywo, chat, ćwiczenia	Wojciech Bobak	13-06-2025	12:15	13:30	01:15
13 z 13 Walidacja usługi - test teoretyczny z wynikiem generowanym automatycznie	Wojciech Bobak	13-06-2025	13:30	13:45	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 800,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	164,71 PLN
Koszt osobogodziny netto	164,71 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wojciech Bobak

Specjalista z zakresu IT Security z ponad 10 letnim doświadczeniem, prelegent wielu konferencji, podcastów oraz wywiadów z zakresu bezpieczeństwa w IT dla młodzieży i dorosłych w tym klientów korporacyjnych. Administrator systemów informatycznych z wszechstronną wiedzą z zakresu zarządzania sieciami oraz systemami IT. Nauczyciel akademicki WSB-NLU, opiekun specjalności pod nazwą Analityk Cyberbezpieczeństwa, koordynator projektu "IT Sec for YOU".
Swoją pracę skupia na pasji oraz ciągłym rozwoju, podczas zajęć akademickich stosuje się do motto „Dobry nauczyciel uczy, świetny nauczyciel inspiruje” tym samym zdobywając uznanie wśród swoich podopiecznych. Obszar zainteresowań: Rekonesans, audyt oraz testy penetracyjne

infrastruktury IT i oprogramowania; Biały wywiad OSINT; Analiza powłamaniowa; Bezpieczeństwo IoT; Bezpieczeństwo/Hardening systemów oraz sieci komputerowych; Systemy operacyjne; Sieci komputerowe; Organizacja i architektura komputerów; Rozwiązania IoT/Monitoringu wizyjnego. Szkoli m. in. z bezpieczeństwa cyfrowego. Posiada doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat od dnia rozpoczęcia szkolenia. Wykształcenie: wyższe. bobak.wojciech@gmail.com

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt szkoleniowy, ankieta, test.

Informacje dodatkowe

- Po szkoleniu uczestnik otrzyma zaświadczenie.
- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie zajęć w formie testu.
- 1 godzina rozliczeniowa = 45 minut dydaktycznych.
- Szkolenie trwa 17 godzin dydaktycznych.
- Zwolnienie z VAT na podstawie § 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 (tekst jednolity Dz.U. z 2020r., poz. 1983).
- Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”.

Warunki techniczne

Forma zdalna usługi. Szkolenie odbywa się za pomocą platformy ZOOM.US.

1. W celu prawidłowego i pełnego korzystania ze szkolenia, Uczestnik powinien dysponować:

- urządzeniem mającym dostęp do sieci Internet (komputer, smartfon, tablet),
- zdolnym do odbioru i przekazu dźwięku (głośniki, słuchawki, mikrofon), przeglądarką Windows: IE 11+, Edge 12+, Firefox 27+, Chrome 30+, Mac: Safari 7+, Firefox 27+, Chrome 30+.
- kamerką internetową.

2. Minimalna wymagana szybkość połączenia internetowego w celu korzystania z webinariów wynosi 2 Mb/s (zalecane połączenie szerokopasmowe).

3. Dołączenie następuje poprzez kliknięcie w indywidualny link wysłany mailem do uczestnika przed szkoleniem oraz wpisanie imienia i nazwiska w oknie logowania.

4. Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych, w tym m in. w zakresie powierzania usług.

Ważność linku - od rozpoczęcia szkolenia do jego zakończenia zgodnie z harmonogramem w karcie.

Kontakt

Ewa Wąsowicz

E-mail ewa.wasowicz@spatiumdg.pl
Telefon (+48) 733 250 350