Możliwość dofinansowania

[CYBER]bezpieczny pracownik - specjalista ds. cyberbezpieczeństwa organizacji

Numer usługi 2026/02/03/7392/3303089

5 200,00 PLN brutto
5 200,00 PLN netto
108,33 PLN brutto/h
108,33 PLN netto/h

Zakład Doskonalenia Zawodowego

4,7 / 5

5 154 oceny

Poznań
Usługa szkoleniowa
stacjonarna
48:00 h
18.05.2026 do 05.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Kurs przeznaczony jest dla pracowników zainteresowanych zwiększeniem świadomości oraz kompetencji z zakresu cyberbezpieczeństwa oraz higieny cyfrowej.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	17-05-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	48
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Zrozumienie i umiejętność praktycznego zastosowania technik obrony przed podstawowymi cyberzagrożeniami, z którymi uczestnik może spotkać się zarówno podczas pracy jak i w życiu codziennym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia podstawowe zagrożenia związane z cyberbezpieczeństwem i uzasadnia potrzebę stosowania higieny cyfrowej.	Definiuje kluczowe pojęcia związane z cyberbezpieczeństwem.	Test teoretyczny
	Ocenia wpływ różnych zagrożeń w sieci organizację.	Test teoretyczny
	Definiuje podstawowe terminy związane z cyberbezpieczeństwem.	Test teoretyczny
	Charakteryzuje podstawowe zasady higieny cyfrowej.	Test teoretyczny
	Charakteryzuje wymagania stawiane przez różne regulacje i normy, wskazując na ich znaczenie dla organizacji.	Test teoretyczny
Strosuje techniki ochrony przed cyberzagrożeniami.	Stosuje zasady bezpiecznego korzystania z przeglądarek internetowych i wyszukiwarek.	Obserwacja w warunkach rzeczywistych
	Monitoruje swoje transakcje bankowe i e-commerce pod kątem nieautoryzowanych działań.	Obserwacja w warunkach rzeczywistych
	Stosuje środki ochorony przed phishingiem i ransomware.	Obserwacja w warunkach rzeczywistych
	Stosuje bezpieczne hasła oraz mechanizmy dwuetapowej weryfikacji.	Obserwacja w warunkach rzeczywistych
	Monitoruje urządzenia używane do pracy zdalnej, upewniając się, że są one zabezpieczone i zgodne z politykami bezpieczeństwa organizacji.	Obserwacja w warunkach rzeczywistych

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

1. Wprowadzenie do cyberbezpieczeństwa

- Kluczowa rola specjalisty ds. cyberbezpieczeństwa w organizacji
- Aktualne zagrożenia cybernetyczne – przegląd i analiza
- Cyberbezpieczeństwo jako element strategii biznesowej

2. Cyberzagrożenia w codziennej pracy

- Ataki phishingowe i socjotechniczne – jak je rozpoznawać?
- Ransomware, malware, DDoS – mechanizmy działania
- Błędy ludzkie jako główna przyczyna incydentów

3. Podstawowe zasady cyberhigieny

- Tworzenie i zarządzanie bezpiecznymi hasłami
- Zasady bezpiecznej pracy zdalnej i BYOD (Bring Your Own Device)
- Bezpieczne korzystanie z poczty e-mail i Internetu

4. 🔍 WARSZTAT: Obrona przed inżynierią społeczną

- Przykłady realnych ataków socjotechnicznych
- Symulacja phishingu – analiza podejrzanych wiadomości
- Techniki manipulacji – jak unikać oszustw?

5. Ochrona danych i infrastruktury IT

- Kluczowe polityki bezpieczeństwa IT w firmie
- Zarządzanie dostępami i kontrola uprawnień
- Bezpieczne przechowywanie i przesyłanie danych

6. 🛡️ SELFTEST: Twoja świadomość cyberbezpieczeństwa

- Test sprawdzający wiedzę i nawyki bezpieczeństwa
- Indywidualna ocena poziomu ryzyka
- Rekomendacje poprawy cyberhigieny

7. Reagowanie na incydenty cybernetyczne

- Jak rozpoznać, zgłosić i reagować na ataki?
- Procedury i standardy postępowania w organizacji
- Współpraca z zespołami IT i zarządem w sytuacji kryzysowej

8. Narzędzia i technologie wspierające cyberbezpieczeństwo

- Oprogramowanie ochronne i systemy monitorujące
- MFA (Multi-Factor Authentication) i VPN – dlaczego są ważne?
- Sztuczna inteligencja i automatyzacja w cyberobronie

9. Budowanie kultury cyberbezpieczeństwa w organizacji

- Jak edukować pracowników i podnosić świadomość?
- Wdrażanie polityk bezpieczeństwa IT
- Case studies: skuteczne strategie w firmach

10. Podsumowanie i sesja Q&A

- Kluczowe wnioski dla specjalistów ds. cyberbezpieczeństwa
- Rekomendacje i dobre praktyki
- Odpowiedzi na pytania uczestników

11. Praktyczne aspekty analizy incydentów cybernetycznych

- Studium przypadku ataków na firmy (analiza realnych incydentów)
- Jak analizować logi systemowe i identyfikować nieautoryzowaną aktywność?
- Wykorzystanie narzędzi SIEM (np. Splunk, ELK)

12. Cyberbezpieczeństwo w chmurze i IoT

- Specyfika zagrożeń w środowiskach chmurowych (AWS, Azure, Google Cloud)
- Jak zabezpieczyć urządzenia IoT w firmie?
- Praktyczne ćwiczenia: konfiguracja bezpiecznej chmury

13. 🔍 WARSZTAT: Testy penetracyjne i podstawy etycznego hackingu

- Jak myśli haker? Wprowadzenie do metod ataku
- Podstawowe narzędzia do testów penetracyjnych (np. Kali Linux, Metasploit)
- Symulacja ataku na słabe hasła i złe konfiguracje systemów

14. Bezpieczeństwo aplikacji i DevSecOps

- Jakie błędy popełniają programiści? OWASP Top 10
- Wdrożenie zasad Secure Coding
- Integracja bezpieczeństwa w cyklu życia oprogramowania (CI/CD)

15. Przyszłość cyberbezpieczeństwa – nowe zagrożenia i trendy

- AI i cyberbezpieczeństwo – jak sztuczna inteligencja pomaga i szkodzi?
- Deepfake, ataki na blockchain i inne nowoczesne zagrożenia
- Jakie umiejętności warto rozwijać w przyszłości?

16. Certyfikacja i ścieżka kariery w cyberbezpieczeństwie

- Przegląd certyfikatów (CompTIA Security+, CISSP, CEH, CISM)
- Jak budować swoją pozycję jako specjalista ds. cyberbezpieczeństwa?
- Rekomendowane dalsze kroki i materiały do nauki

17. Egzamin KCA

Warunki organizacyjne: Szkolenie prowadzone jest w 1 grupie szkoleniowej, na 1 osobę przypada jedno stanowisko komputerowe.

Usługa szkoleniowa realizowana jest w godzinach dydaktycznych. Na każde zajęcia przewidziano 15-minutową przerwę.

Egzamin przeprowadzany jest przez podmiot zewnętrzny i jest realizowany w godzinach zegarowych.

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 200,00 PLN
Koszt przypadający na 1 uczestnika netto	5 200,00 PLN
Koszt osobogodziny brutto	108,33 PLN
Koszt osobogodziny netto	108,33 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały drukowane

Warunki uczestnictwa

- umiejętność obsługi komputera

Informacje dodatkowe

Uwaga! W przypadku liczby chętnych mniejszej niż 8 osób, Zakład Doskonalenia Zawodowego zastrzega sobie prawo do odwołania lub przeniesienia terminu kursu.

Adres

ul. Metalowa 4

60-112 Poznań

woj. wielkopolskie

Każdemu uczestnikowi przypisane jest jedno stanowisko komputerowe.

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Judyta Serwecińska

E-mail judyta.serwecinska@zdz.poznan.pl

Telefon (+48) 605 454 141