



Cyberbezpieczeństwo - narzędzia i strategię umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami. Szkolenie i konsultacje.

Numer usługi 2026/08/05/8282/3731184

2 078,70 PLN brutto

1 690,00 PLN netto

173,23 PLN brutto/h

140,83 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Centrum Organizacji

Szkoleń i

Konferencji SEMPER

Magdalena

Wolniewicz-Kesaria

★★★★☆ 4,5 / 5

3 204 oceny

🏠 Usługa szkoleniowa

📄 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 12:00 h

📅 27.09.2027 do 28.09.2027

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

1. Pracownicy działów IT i informatycy odpowiedzialni za bezpieczeństwo systemów informatycznych.
2. Specjaliści ds. bezpieczeństwa informacji i cyberbezpieczeństwa.
3. Kierownictwo i kadra zarządzająca, odpowiedzialna za podejmowanie decyzji dotyczących bezpieczeństwa cybernetycznego.
4. Specjaliści zainteresowani rozwojem zawodowym w dziedzinie cyberbezpieczeństwa.
5. Wszystkie osoby zainteresowane omawianą podczas szkolenia tematyką.

Minimalna liczba uczestników

2

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji

26-09-2027

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

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

Zwiększenie świadomości na temat cyberbezpieczeństwa wśród uczestników.

Zdobycie wiedzy teoretycznej i praktycznych umiejętności z zakresu cyberbezpieczeństwa.

Wypożyczenie uczestników w narzędzia i strategię umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami cybernetycznymi.

Promowanie postaw odpowiedzialnego korzystania z technologii i przeciwdziałanie cyberprzestępczości.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kompetencje społeczne: - ocenia jak odpowiednio reagować w różnych sytuacjach związanych z wykonywanym zawodem - identyfikuje własny styl uczenia się i wybiera sposoby dalszego kształcenia, - określa znaczenie komunikacji interpersonalnej oraz potrafi prawidłowo identyfikować i rozstrzygać dylematy związane z wykonywaniem zawodu.	- Umiejętność dostosowania reakcji do różnorodnych kontekstów zawodowych - Wybór adekwatnych metod do dalszego kształcenia.	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Organizator zastrzega sobie prawo do zmiany harmonogramu realizacji usługi. Ostateczne informacje zostaną przekazane uczestnikom najpóźniej na 7 dni przed rozpoczęciem szkolenia. Zmiana harmonogramu nie wpływa na całkowity wymiar godzin szkolenia.

Moduł 1: Podstawy cyberbezpieczeństwa

1. Wprowadzenie do cyberbezpieczeństwa: definicja, znaczenie i aktualne zagrożenia.
2. Rodzaje ataków cybernetycznych: malware, phishing, ransomware, ataki DDoS itp.

- 3. Podstawowe pojęcia związane z cyberbezpieczeństwem: poufność, integralność, dostępność, poufność, niezaprzeczalność.
- 4. Regulatory i standardy związane z cyberbezpieczeństwem: GDPR, ISO 27001.

Moduł 2: Bezpieczeństwo sieci

- 1. Zagrożenia związane z sieciami komputerowymi.
- 2. Architektura sieciowa i zasady projektowania bezpiecznej sieci.
- 3. Firewall: rodzaje, konfiguracja i zarządzanie nimi.
- 4. Zabezpieczanie sieci bezprzewodowych: uwierzytelnianie, szyfrowanie, filtrowanie adresów MAC.
- 5. Zarządzanie hasłami i autoryzacją: zasady tworzenia silnych haseł, zarządzanie kontami użytkowników.

Moduł 3: Bezpieczeństwo systemów operacyjnych

- 1. Aktualizacje systemów operacyjnych i aplikacji: znaczenie i procedury.
- 2. Antywirusy i antimalware: instalacja, konfiguracja i skanowanie systemu.
- 3. Bezpieczne korzystanie z systemu: zasady tworzenia kont użytkowników, zarządzanie uprawnieniami.
- 4. Monitorowanie systemu: logi, analiza zdarzeń bezpieczeństwa, wykrywanie nieprawidłowości.

Moduł 4: Bezpieczeństwo aplikacji

- 1. Testowanie penetracyjne: zasady, narzędzia i techniki.
- 2. Ochrona przed atakami typu SQL injection i cross-site scripting.
- 3. Bezpieczeństwo aplikacji webowych: filtrowanie wejścia, zabezpieczanie sesji, walidacja danych.
- 4. Bezpieczeństwo aplikacji mobilnych: uwierzytelnianie, szyfrowanie danych, zarządzanie uprawnieniami.

Moduł 5: Zarządzanie incydentami i reagowanie na ataki

- 1. Planowanie reakcji na incydenty: tworzenie procedur, zespoły odpowiedzialne za reagowanie.
- 2. Analiza zdarzeń bezpieczeństwa: narzędzia i techniki identyfikacji i analizy ataków.
- 3. Reagowanie na incydenty: odizolowanie systemów, odzyskiwanie danych, przywracanie działania.
- 4. Audyt bezpieczeństwa: przegląd systemów, ocena zgodności z zasadami bezpieczeństwa.

Moduł 6: Polityka bezpieczeństwa i świadomość użytkowników

- 1. Tworzenie polityki bezpieczeństwa: cele, zasady i procedury.
- 2. Szkolenia dla pracowników: edukacja w zakresie bezpiecznego korzystania z technologii.
- 3. Zarządzanie ryzykiem: ocena ryzyka, zarządzanie incydentami, planowanie ciągłości działania.
- 4. Bezpieczeństwo w chmurze: zagrożenia i najlepsze praktyki związane z usługami chmurowymi.

Program szkolenia będzie obejmował zarówno wykłady teoretyczne, jak i praktyczne warsztaty, w których uczestnicy będą mieli okazję zastosować zdobytą wiedzę w praktyce. Podczas szkolenia będą używane różne narzędzia i symulacje, aby umożliwić uczestnikom eksplorację rzeczywistych scenariuszy i sytuacji związanych z cyberbezpieczeństwem.

Prosimy o traktowanie liczby zapisów widocznych w BUR wyłącznie orientacyjnie. Rejestracje poprzez BUR są tylko częścią zapisów na szkolenie, ponieważ prowadzimy również nabór komercyjny, którego liczba uczestników nie jest widoczna w systemie BUR. Zachęcamy do rezerwacji miejsca - grupy szkoleniowe są tworzone również na podstawie zapisów spoza BUR

Harmonogram

Liczba pozycji harmonogramu: 5

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Cyberbezpieczeństwo	Zajęcia	Trener Semper	27-09-2027	09:00	14:00	05:00
2 z 5 -	Przerwa	-	27-09-2027	14:00	15:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 5 Cyberbezpieczeństwo	Zajęcia	Trener Semper	28-09-2027	09:00	13:00	04:00
4 z 5 -	Przerwa	-	28-09-2027	13:00	14:00	01:00
5 z 5 -	Walidacja	-	28-09-2027	14:00	15:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	12:00
w tym suma godzin zajęć	09:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	13:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeżeli usługa w całości jest finansowana ze środków publicznych lub § 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, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 078,70 PLN
Koszt przypadający na 1 uczestnika netto	1 690,00 PLN
Koszt osobogodziny brutto	173,23 PLN
Koszt osobogodziny netto	140,83 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	12:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Trener Semper

Ekspert Centrum Organizacji Szkoleń i Konferencji SEMPER

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- materiały szkoleniowe w wersji elektronicznej
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu

Warunki uczestnictwa

ZGŁOSZENIE NA USŁUGĘ

Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

Dla jednostek budżetowych finansujących udział w szkoleniu w minimum 70% lub w całości ze środków publicznych stawka podatku VAT = zw.

Informacje dodatkowe

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z Internetem (komputer, tablet, telefon), słuchawki lub głośniki i ulubiony fotel
- szkolenie realizowane jest w nowoczesnej formie w wirtualnym pokoju konferencyjnym i kameralnej grupie uczestników
- bierzesz udział w pełnowartościowym szkoleniu - Trener prowadzi zajęcia "na żywo" - widzisz go i słyszysz
- pokaz prezentacji, ankiet i ćwiczeń widzisz na ekranie swojego komputera w czasie rzeczywistym.
- podczas szkolenia Trener aktywizuje uczestników zadając pytania, na które można odpowiedzieć w czasie rzeczywistym
- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu

Warunki techniczne

Wymagania techniczne:

- Platforma /rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa - Platforma Zoom (<https://zoom-video.pl/>)

Wymagania sprzętowe:

- Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji - komputer, laptop lub inne urządzenie z dostępem do internetu
- Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik - minimalna prędkość łącza: 512 KB/sek
- Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów - komputer, laptop lub inne urządzenie z dostępem do internetu. Nie ma potrzeby instalowania specjalnego oprogramowania.
- Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line - od momentu rozpoczęcia szkolenia do momentu zakończenia szkolenia
- Potrzebna jest zainstalowana najbardziej aktualna oficjalna wersja jednej z przeglądarek: Google Chrome, Mozilla Firefox, Safari, Edge lub Opera. 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, Chrome OS. Łącze internetowe o minimalnej przepustowości do zapewnienia transmisji dźwięku 512Kb/s, zalecane

Kontakt



Angelika Poznańska

E-mail info@szkolenia-semper.pl

Telefon (+48) 570 590 060