



| Nr części i nazwa szkolenia   | Założenia organizacyjne/ zakres programowy szkolenia   | Efekty uczenia   | Liczba godzin/ liczba uczestników(-czek)   | Minimalne wymagania dla wykładowcy/ trenera   |
|---|--|--|--|---|
| <b>CZĘŚĆ 1</b><br><b>Certified Ethical Hacker AI wraz z egzaminem EC-COUNCIL</b><br><b>(lub o równoważnej uznawalności)</b> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <ol style="list-style-type: none"> <li>1. Wprowadzenie do etycznego hakingu</li> <li>2. Zbieranie informacji o ataku</li> <li>3. Skanowanie sieci</li> <li>4. Hackowanie systemu</li> <li>5. Złośliwe oprogramowanie</li> <li>6. Monitorowanie i przechwytywanie danych</li> <li>7. Inżynieria społeczna – socjotechniki</li> <li>8. Przejęcie sesji</li> <li>9. Hakowanie serwerów sieciowych</li> <li>10. Hakowanie aplikacji internetowych</li> <li>11. Hakowanie mobilnych platform</li> <li>12. Hakowanie Internetu Rzeczy</li> <li>13. Bezpieczeństwo chmury</li> </ol> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć najnowocześniejsze umiejętności oparte na sztucznej inteligencji, zwiększając zdolność do wykonywania zadań związanych z zapewnieniem cyberbezpieczeństwa .</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w szczególności z uwzględnieniem cyberbezpieczeństwa .</p> <p>Jednocześnie nabyte kompetencje uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie go do potrzeb studentów i potrzeb współczesnego rynku pracy.</p> <p>Szkolenie musi zakończyć się certyfikującym egzaminem, który potwierdzi nabycie</p> | <p>Liczba uczestników (-czek): 2 osoby</p> <p>Minimalna liczba godzin pełnego szkolenia:</p> <p>35 h dydaktycznych</p> <p>Lokalizacja:</p> <p>Online lub inna</p> <p>Termin realizacji pełnego szkolenia z egzaminem:</p> <p>Styczeń 2025 r. – maj 2026 r.</p> | <ul style="list-style-type: none"> <li>• min. wykształcenie wyższe (min. licencjat),</li> <li>• min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>• w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 35 godzin dydaktycznych każde szkolenie.</li> </ul> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2 referencje, protokoły, zaświadczenia lub inne równoważne dokumenty wystawione przez min. 2 różne podmioty w dwóch różnych terminach.</p> <p>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</p> |



|  |   |   |  |   |
|--|---|---|--|---|
|  | 14. Kryptografia  | kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.<br><br>Wykonawca powinien zapewnić taki zakres szkolenia aby uczestnik (-czka) w pełni przygotował się do egzaminu certyfikującego.<br><br>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.  |  |   |
| <b>CZĘŚĆ 2</b><br><b>Certified Information Systems Security Professional wraz z egzaminem CISSP (lub o równoważnej uznawalności)</b> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu</li> <li>2. Ataki w obszarze kontroli dostępu i monitorowanie</li> <li>3. Bezpieczna architektura i zabezpieczanie komponentów sieci</li> <li>4. Bezpieczna komunikacja i ataki sieciowe</li> </ol> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć eksperckie umiejętności w dziedzinie bezpieczeństwa informacji.</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w szczególności z uwzględnieniem cyberbezpieczeństwa</p> <p>Jednocześnie nabyte kompetencje uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie go do potrzeb studentów i potrzeb współczesnego rynku pracy.</p> | <p>Liczba uczestników (-czek): 1 osoba</p> <p>Minimalna liczba godzin pełnego szkolenia:</p> <p>35 h dydaktycznych</p> <p>Lokalizacja:</p> <p>Online lub inna</p> <p>Termin realizacji pełnego szkolenia z egzaminem:</p> <p>Styczeń 2025 r. – maj 2026 r.</p> | <ul style="list-style-type: none"> <li>• min. wykształcenie wyższe (min. licencjat),</li> <li>• min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>• w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 35 godzin dydaktycznych każde szkolenie.</li> </ul> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2 referencje, protokoły, zaświadczenia lub inne równoważne dokumenty wystawione przez min. 2 różne podmioty w</p> |



|   |  |  |   |  |
|---|--|--|---|--|
|   | <p>5. Bezpieczeństwo związane z rozwojem oprogramowania</p> <p>6. Kod złośliwy i ataki na aplikacje</p> <p>7. Kryptografia i algorytmy kluczy symetrycznych</p> <p>8. Infrastruktura PKI i aplikacje kryptograficzne</p> <p>9. Bezpieczeństwo działalności operacyjnej</p> <p>10. Zarządzanie incydentami</p>  | <p>Szkolenie musi zakończyć się certyfikującym egzaminem, który potwierdzi nabycie kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.</p> <p>Wykonawca powinien zapewnić taki zakres szkolenia aby uczestnik (-czka) w pełni przygotował się do egzaminu certyfikującego.</p> <p>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.</p>  |   | <p>dwóch różnych terminach.</p> <ul style="list-style-type: none"> <li>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</li> </ul>  |
| <p><b>CZĘŚĆ 3</b></p> <p><b>FortiOS/Forti Gate wraz z egzaminem Fortinet Network Security Expert (lub o równoważnej uznawalności)</b></p> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <p>1. Ustawienia systemowe i sieciowe</p> <p>2. Zasady zapory sieciowej i NAT</p> <p>3. Uwierzytelnianie zapory sieciowej</p> <p>4. Logowanie jednokrotne</p> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć specjalistyczne umiejętności w zakresie bezpieczeństwa sieci.</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w szczególności z uwzględnieniem cyberbezpieczeństwa</p> <p>Jednocześnie nabyte kompetencje uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie</p> | <p>Liczba uczestników (-czek): 2 osoby</p> <p>Minimalna liczba godzin pełnego szkolenia: 22 h dydaktycznych</p> <p>Lokalizacja: Online lub inna</p> <p>Termin realizacji pełnego szkolenia z egzaminem: Styczeń 2025 r. – maj 2026 r.</p> | <ul style="list-style-type: none"> <li>min. wykształcenie wyższe (min. licencjat),</li> <li>min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 22 godzin dydaktycznych każde szkolenie.</li> </ul> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2 referencje, protokoły,</p> |



|   |  |  |  |  |
|---|--|--|--|--|
|   | <p>5. Operacje certyfikatów</p> <p>6. Zapobieganie włamaniom i kontrola aplikacji</p> <p>7. Diagnozowanie i rozwiązywanie problemów</p> <p>8. Sieć VPN IPsec</p>   | <p>go do potrzeb studentów i potrzeb współczesnego rynku pracy.</p> <p>Szkolenie musi zakończyć się certyfikującym egzaminem, który potwierdzi nabycie kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.</p> <p>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.</p>  |  | <p>zaświadczenia lub inne równoważne dokumenty wystawione przez min. 2 różne podmioty w dwóch różnych terminach.</p> <p>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</p>  |
| <p><b>CZĘŚĆ 4</b></p> <p><b>Linux System Administrator (LFCS). (lub o równoważnej uznawalności)</b></p> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <p>1. Układ drzewa systemu plików Linux</p> <p>2. Zarządzanie kontami użytkowników</p> <p>3. Uprawnienia i własność plików</p> <p>4. Systemy zarządzania</p> <p>5. Podstawy GIT</p> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć specjalistyczne umiejętności w zakresie administrowania systemu Linux.</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w szczególności z uwzględnieniem cyberbezpieczeństwa.</p> <p>Jednocześnie nabyte kompetencje uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie go do potrzeb studentów i potrzeb</p> | <p>Liczba uczestników (-czek): 2 osoby</p> <p>Minimalna liczba godzin pełnego szkolenia:</p> <p>22 h dydaktycznych</p> <p>Lokalizacja:</p> <p>Online lub inna</p> <p>Termin realizacji pełnego szkolenia z egzaminem:</p> <p>Styczeń 2025 r. – maj 2026 r.</p> | <ul style="list-style-type: none"> <li>min. wykształcenie wyższe (min. licencjat),</li> <li>min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 22 godzin dydaktycznych każde szkolenie.</li> </ul> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2 referencje, protokoły, zaświadczenia lub inne równoważne dokumenty</p> |



|  |   |   |   |   |
|--|---|---|---|---|
|  | <p>6. Procesy i monitorowanie</p> <p>7. Systemy plików Linux i VFS</p> <p>8. Podział dysków</p> <p>9. Zapory sieciowe</p> <p>10. Moduły bezpieczeństwa Linux</p> <p>11. Odzyskiwanie systemu</p>  | <p>współczesnego rynku pracy.</p> <p>Szkolenie musi zakończyć się certyfikującym egzaminem, który potwierdzi nabycie kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.</p> <p>Wykonawca powinien zapewnić taki zakres szkolenia aby uczestnik (-czka) w pełni przygotował się do egzaminu certyfikującego.</p> <p>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.</p> |   | <p>wystawione przez min. 2 różne podmioty w dwóch różnych terminach.</p> <p>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</p>   |
| <p><b>CZĘŚĆ 5</b></p> <p><b>Machine Learning Engineering on AWS wraz z egzaminem AWS Certified Machine Learning (lub o równoważnej uznawalności)</b></p> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <p>1: Analiza wyzwań uczenia maszynowego</p> <p>2: Przetwarzanie danych dla uczenia maszynowego</p> <p>3: Wybór podejścia do modelowania</p> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć specjalistyczne umiejętności w zakresie uczenia maszynowego (ML) w Amazon Web Services (AWS).</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w szczególności z uwzględnieniem cyberbezpieczeństwa</p> <p>Jednocześnie nabyte kompetencje</p>                   | <p>Liczba uczestników (-czek): 1 osoba</p> <p>Minimalna liczba godzin pełnego szkolenia:</p> <p>22 h dydaktycznych</p> <p>Lokalizacja:</p> <p>Online lub inna</p> <p>Termin realizacji pełnego szkolenia z egzaminem:</p> | <ul style="list-style-type: none"> <li>• min. wykształcenie wyższe (min. licencjat),</li> <li>• min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>• w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 22 godzin dydaktycznych każde szkolenie.</li> </ul> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2</p> |



|  |   |   |  |   |
|--|---|---|--|---|
|  | <p>4: Szkolenie modeli uczenia maszynowego</p> <p>5: Strategie wdrażania modeli</p> <p>6: Zabezpieczanie zasobów uczenia maszynowego</p> <p>7: Monitorowanie wydajności modelu i jakości danych.</p>  | <p>uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie go do potrzeb studentów i potrzeb współczesnego rynku pracy.</p> <p>Szkolenie musi zakończyć się egzaminem, który potwierdzi nabycie kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.</p> <p>Wykonawca powinien zapewnić taki zakres szkolenia aby uczestnik (-czka) w pełni przygotował się do egzaminu certyfikującego.</p> <p>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.</p> | <p>Styczeń 2025 r. – maj 2026 r.</p>   | <p>referencje, protokoły, zaświadczenia lub inne równoważne dokumenty wystawione przez min. 2 różne podmioty w dwóch różnych terminach.</p> <p>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</p>  |
| <p><b>CZĘŚĆ 6</b></p> <p><b>Machine Learning on Google Cloud wraz z egzaminem Google Cloud Certified Professional Machine Learning Engineer (lub o równoważnej uznawalności)</b></p> | <p>Szkolenie kierowane jest do pracowników(-czek) dydaktycznych AWSB, którzy docelowo uzyskają nowe kompetencje dydaktyczne.</p> <p>Szkolenie winno odbywać się w formie stacjonarnej w odległości maksymalnie 100 km od siedziby Zamawiającego lub online. W ofercie należy wskazać formę szkolenia.</p> <p>Minimalny zakres szkolenia:</p> <p>1. Wprowadzenie do sztucznej inteligencji i</p> | <p>Po zakończonym szkoleniu uczestnicy(-czki) szkolenia powinni(y) nabyć specjalistyczne umiejętności w zakresie rozwiązań sztucznej inteligencji (AI) i uczenia maszynowego (ML) w Google Cloud.</p> <p>Szkolenie wpłynie na zwiększenie umiejętności uczestników (-czek) w zakresie specjalistycznych kompetencji cyfrowych, w</p>  | <p>Liczba uczestników (-czek): 1 osoba</p> <p>Minimalna liczba godzin pełnego szkolenia:</p> <p>22 h dydaktycznych</p> <p>Lokalizacja:</p> <p>Online lub inna</p> <p>Termin realizacji</p> | <ul style="list-style-type: none"> <li>• min. wykształcenie wyższe (min. licencjat),</li> <li>• min. 5 letnie doświadczenie w zakresie prowadzenia szkolenia z danego zakresu,</li> <li>• w ciągu ostatnich 3 lat przed upływem terminu składania ofert zrealizował(a) minimum 2 szkolenia z danego zakresu, w wymiarze minimum 22 godzin dydaktycznych każde szkolenie.</li> </ul> |



|  |   |   |  |  |
|--|---|---|--|--|
|  | <p>uczenia maszynowego w Google Cloud</p> <p>2. Inżynieria cech</p> <p>3. Uczenie maszynowe</p> | <p>szczegółowości z uwzględnieniem cyberbezpieczeństwa</p> <p>.</p> <p>Jednocześnie nabyte kompetencje uczestników (-czek) pozwolą na modyfikację procesu dydaktycznego i lepsze dostosowanie go do potrzeb studentów i potrzeb współczesnego rynku pracy.</p> <p>Szkolenie musi zakończyć się egzaminem, który potwierdzi nabycie kompetencji a dla uczestnika (-czki) zostanie wystawiony certyfikat.</p> <p>Wykonawca powinien zapewnić taki zakres szkolenia aby uczestnik (-czka) w pełni przygotował się do egzaminu certyfikującego.</p> <p>Wykonawca zapewni materiały szkoleniowe co najmniej w wersji elektronicznej.</p> | <p>pełnego szkolenia z egzaminem:</p> <p>Styczeń 2025 r. – maj 2026 r.</p> | <p>.</p> <p>W celu potwierdzenia spełnienia warunku należy do oferty dołączyć min. 2 referencje, protokoły, zaświadczenia lub inne równoważne dokumenty wystawione przez min. 2 różne podmioty w dwóch różnych terminach.</p> <p>Dokumenty muszą jednoznacznie wskazywać szkolenie z zakresem na które składana jest oferta.</p> |
|--|---|---|--|--|