Załącznik do formularza oferty

**Zadanie nr 13 – szkolenia z zakresu cyberbezpieczeństwa - 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametry techniczne i funkcjonalne** | **Wymagania graniczne** | **Parametry oferowane**  *(podać zakres lub opisać)* |
|  | Nazwa: | Podać |  |
|  | Producent/model | Podać |  |
|  | Kraj pochodzenia | Podać |  |
|  | Rok produkcji nie starszy niż 2025, urządzenie fabrycznie nowe | Nd. |  |
|  | **PARAMETRY TECHNICZNE I EKSPLOATACYJNE** | | |
|  | Minimalne wymagania funkcjonalne dla platformy szkoleniowej:   * indywidualne konto dla każdego z użytkowników korzystających z platformy * możliwość swobodnego poruszania się pomiędzy poszczególnymi lekcjami i modułami kursu * śledzenie postępów użytkowników poprzez generowanie raportu pokazującego ile lekcji z całości kursu ukończył dany pracownik (opcja ta powinna być dostępna wyłącznie dla wybranych osób) * weryfikacja wiedzy użytkowników, którzy ukończyli poszczególne moduły poprzez quizy (w tym weryfikacja ile razy dany użytkownik rozwiązywał quiz zanim go zdał) * pamiętanie postępów użytkownika w celu umożliwienia mu kontynuacji nauki od miejsca, w którym zakończył sesję z platformą * samodzielna zmiana lub resetowanie hasła w przypadku jego zapomnienia * śledzenie ilości prób logowania i automatyczne blokowanie kont w przypadku przekroczenia zdefiniowanej ilości błędnych logowań * udostępnianie materiału edukacyjnego w dwóch trybach (do wyboru): natychmiastowy dostęp do całości materiału lub poszczególne moduły odkrywane stopniowo (np. raz w tygodniu) * zautomatyzowana wysyłkę powiadomień do użytkowników z przypomnieniem o konieczności zapoznania się z kolejnymi modułami * generowanie certyfikatów w formie PDF przez użytkowników, którzy pomyślnie rozwiązali wszystkie quizy * mechanizm hurtowego importu dużej liczby użytkowników do platformy * dostępność z dowolnego urządzenia z przeglądarką internetową (responsywność strony) bez konieczności instalacji dodatkowych aplikacji | TAK/opis |  |
|  | Platforma powinna uwzględniać potrzeby osób niepełnosprawnych, w tym m.in.:   * możliwość dostosowania (zwiększania, zmniejszania) rozmiaru czcionek * możliwość wyboru jednej z wersji kolorystycznych (szarości, wysoki kontrast, negatyw, jasne tło) * możliwość włączenia trybu podkreślania linków * możliwość włączenia trybu czytelnych czcionek | TAK/opis |  |
|  | Platforma powinna spełniać wymogi RODO dotyczące bezpieczeństwa, przechowywania danych osobowych na terenie Europejskiego Obszaru Gospodarczego oraz minimalizacji zakresu i czasu przetwarzania danych osobowych. Dostawca platformy zobowiązany jest przeprowadzać w formie udokumentowanej analizę ryzyka związanego z bezpieczeństwem danych osobowych minimum raz w roku oraz przy każdej zmianie mogącej mieć istotny wpływ na bezpieczeństwo danych osobowych. | TAK/opis |  |
|  | Minimalne wymagania dotyczące treści edukacyjnych:   * Materiały szkoleniowe powinny mieć format wideo-wykładów z udziałem wykładowcy omawiającego poszczególne zagadnienia (niedopuszczalne są nagrania generowane z udziałem sztucznej inteligencji nawet w przypadku realistycznie wyglądających postaci, a także lekcje składające się wyłącznie z animacji) * Lekcje prowadzone powinny być przez praktyków z minimum 5. letnim doświadczeniem zawodowym w obszarze cyberbezpieczeństwa. Doświadczenie to poparte powinno być referencjami oraz posiadaniem minimum jednego z certyfikatów branżowych (CEH, OSCP, LPT) * Wykłady poparte powinny być dużą ilością realnych przykładów zagrożeń * Lekcje powinny być wzbogacone materiałami dodatkowymi w postaci dokumentów, nagrań, opracowań * Poza prezentacjami i przykładami praktycznymi na materiał powinny się składać filmy instruktażowe prezentujące realne zastosowania narzędzi podnoszących bezpieczeństwo. * Materiały wideo powinny być prezentowane z dedykowanej platformy gwarantującej wysoką dostępność i wydajność, która nie osadza w treści wideo dodatkowych elementów typu reklamy, polecenia, playlisty, odnośniki do zewnętrznych materiałów. * Materiały edukacyjne powinny mieć spójny charakter i być przygotowane oraz zaprezentowane przez jednego wykładowcę. Niedopuszczalna jest kompilacja treści pochodzących z różnych źródeł. * Treści edukacyjne nie powinny zawierać lokowania produktów oraz płatnych promocji, w tym linków afiliacyjnych. * Treści powinny być prezentowane w języku polskim (niedopuszczalne jest stosowanie treści obcojęzycznych z tłumaczeniem w postaci napisów) | TAK/opis |  |
|  | Wymagania odnośnie zakresu tematycznego i czasu trwania lekcji:   * łączny czas trwania lekcji w platformie powinien przekraczać 7 pełnych godzin zegarowych * zakres tematyczny kursu powinien obejmować minimum: * zagrożenia socjotechniczne (scam, phishing, smshing, spoofing, złośliwe reklamy) * bezpieczeństwo haseł (przykłady stosowania, złe i dobre praktyki, menedżery haseł z instrukcją ich użytkowania, wycieki haseł, reakcja na wyciek hasła) * omówienie zagadnień związanych ze środowiskiem cyberprzestępców oraz darknetem i powodów dla których stanowią oni zagrożenie * omówienie zagadnień uwierzytelniania dwuskładnikowego, w tym z wykorzystaniem kluczy sprzętowych * bezpieczeństwo poczty (złośliwe linki i załączniki, zasady weryfikacji, narzędzia pomagające zweryfikować załącznik takie jak VirusTotal z pokazem użytkowania) * naukę rozpoznawania fałszywych domen i adresów URL z uwzględnieniem zagadnień takich jak typosquatting, cybersquatting * naukę weryfikacji zabezpieczeń strony www (szyfrowanie ssl, certyfikat, dane na certyfikacie, ostrzeżenia o błędach certyfikatu) * bezpieczeństwo przeglądarek (ciasteczka, zapamiętywanie haseł, ataki typu clickjacking, likejacking, camjacking) * zagrożenia związane z urządzeniami (telefony nieznanego pochodzenia, nośniki danych, dedykowane urządzenia hackerskie typu implanty, badusb, urządzenia do przechwytywania i kopiowania sygnałów radiowych oraz zabezpieczeń) * zagrożenia typu SIMswap, ataki techniką wodopoju, ataki telefoniczne, spoofing numeru telefonu * zagrożenia związane z sieciami WiFi * oszustwa wykorzystujące sztuczną inteligencję do generowania obrazu i głosu znanych osób * zagrożenia związane z tzw. Internetem rzeczy i urządzeniami codziennego użytku * zagrożenia związane z fake newsami i dezinformacją * bezpieczeństwo mediów społecznościowych (kradzieże profili, wyłudzanie płatności Blik, podszywanie się pod znane osoby, metody zabezpieczania profili, fałszywe konkursy) * OSINT i metadane oraz prywatność w Internecie * bezpieczeństwo płatności w Internecie (karty płatnicze, bramki płatnicze, Blik, bankowość mobilna) * zagrożenia dla organizacji takie jak szpiegostwo gospodarcze / wrogi pracownik * dobre praktyki bezpieczeństwa (hardening, aktualizacje, ochrona antywirusowa, zapora, kopie bezpieczeństwa, bezpieczne usuwanie danych) * zagrożenia urządzeń mobilnych (złośliwe aplikacje, uprawnienia aplikacji, inwigilacja z użyciem telefonu, bezpieczeństwo dzieci) * rozpoznawanie, zgłaszanie i prawidłowe reagowanie na incydenty bezpieczeństwa * metody zwiększania bezpieczeństwa i poufności komunikacji (zalecana przeglądarka, komunikator, konto pocztowe, vpn, blokada usług premium) * Każdy moduł tematyczny zakończony powinien zostać zadaniem do wykonania przez użytkownika. Celem zadania powinno być utrwalenie materiału zawartego w kursie oraz podniesienie poziomu bezpieczeństwa użytkownika. | TAK/opis |  |
|  | Wymagania dotyczące dedykowanego modułu dla kierownictwa   * Materiały edukacyjne powinny obejmować dodatkowy moduł dedykowany dla kierownictwa organizacji. Moduł ten powinien obejmować minimum tematykę: * Podstaw prawnych w obszarze cyberbezpieczeństwa * Typów ataków * Reagowania na incydenty * Wykonywania badań bezpieczeństwa * Roli kadry zarządzającej w procesach bezpieczeństwa | TAK/opis |  |
|  | 12 miesięcy subskrypcji | TAK |  |

……………………………….

(podpis/popisy osoby/osób upoważnionej/upoważnionych

do reprezentowania wykonawcy)