nr zapytania ofertowego 7/KON/z045/2021

Załącznik nr 1 do Warunków

Specyfikacja

Wymogi dla specjalistycznego oprogramowania komputerowego - symulatora zagrożeń internetowych pozwalającego na utworzenie symulowanej sieci Internet wraz z kreowanymi w niej sztucznie zagrożeniami

Oferta Wykonawcy musi uwzględniać licencję bezterminową niewyłączną na oprogramowanie zawierające przedmiotowy symulator o tematyce wskazanej w niniejszej Specyfikacji.

W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy, poprzez zainstalowanie na serwerze w chmurze specjalistycznego oprogramowania komputerowego dla symulatora zagrożeń internetowych pozwalającego na utworzenie symulowanej sieci Internet wraz z kreowanymi w niej sztucznie zagrożeniami – licencja bezterminowa niewyłączna.

1. Licencja na oprogramowanie musi umożliwiać dostęp do symulatora zagrożeń internetowych przeznaczonego dla nieograniczonej liczby uczestników (użytkowników) szkolących się w celu zdobycia wiedzy o cyberzagrożeniach i praktycznych umiejętności w zakresie rozpoznawania symptomów zachowań przestępczych w Internecie.
2. Licencja na oprogramowanie musi zawierać minimum symulację: mechanizmu ataku phishing, mechanizmu ataku pharming oraz podstawowych zagrożeń dotyczących oprogramowania typu malware.
3. W przygotowaniu projekt narzędzia oraz jego testach powinni uczestniczyć praktycy/eksperci odpowiedzialni za cyberbezpieczeństwo w różnych instytucjach
4. Architektura oprogramowania powinna być:
    a. sieciowa, umożliwiająca uczestnikom korzystanie z symulatora zdalnie
    b. przygotowana w taki sposób aby podstawowa wersji symulatora dawała możliwość stworzenia dodatkowych modułów bez konieczności zmiany fragmentów trwałych (serwera, ustawień firewall, DNS, baz danych, etc.) dając możliwość rozszerzenia zakresu objętych nauczaniem zagadnień.
5. Odpowiedzialność producenta oprogramowania za skutki błędów w programie.
6. W ramach udzielonej licencji bezterminowej Wykonawca zobowiązany do:
    a. wykonania sieci oraz analizy technologicznej,
    b. wykonania dokumentacji technicznej,
    c. wykonania projektu oprogramowania,
    d. przygotowania środowiska oraz implementacja oprogramowania
    e. testów po wdrożeniu,
    f. audytu bezpieczeństwa w wersji skróconej
    g. wdrożenia systemu oraz jego konserwacji,
    h. aktualizacji oprogramowania do 31.12.2021
7. Ponad to w ramach udzielonej licencji bezterminowej Wykonawca zobowiązany do jest przekazać Zamawiającemu:
    a. Regulamin ogólny symulatora
    b. Podręcznik trenera
    c. Prezentację wprowadzającą (w formie pliku Microsoft Power Point)
    d. Skróconą instrukcję gracza
    e. Inne materiały tj.: wzory certyfikatów uczestnictwa.
8. Oprogramowanie zostanie zainstalowane:

NOWY WYMIAR STUDIOWANIA w WSPIA
PROJEKT „NOWY WYMIAR STUDIOWANIA W WSPIA”
PROJEKT WSPÓŁFINANSOWANY ZE ŚRODKÓW EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO
W RAMACH PROGRAMU OPERACYJNEGO WIEDZA EDUKACJA I ROZWÓJ 2014-2020
PROJEKT NR POWR.03.05.00-00-z045/17

nr zapytania ofertowego 7/KON/z045/2021

a. na komputerach Zamawiającego lub studentów z dostęp do sieci lokalnej wyposażonych w system operacyjny Windows z możliwością uruchomienia dostarczonych aplikacji będących w zasobach Zamawiającego.
b. na serwerze w chmurze wraz z zainstalowanym oprogramowaniem - CTS jako SaaS.

Symulator zagrożeń internetowych – opis dodatkowy

- Symulator zagrożeń internetowych wraz z kreowanymi w niej sztucznie zagrożeniami powinien mieć właściwości odpowiadające rzeczywistym niebezpieczeństwom w Internecie. Symulator ma umożliwiać w bezpieczny sposób zdobywanie wiedzy o cyberzagrożeniach. Wykorzystanie tego narzędzia w procesie dydaktycznym ma dać możliwość przekazania studentom praktycznej wiedzy na temat zagrożeń takich jak phising, pharming, malaware i wiele innych w codziennym korzystaniu z technologii internetowych zarówno przez instytucje publiczne oraz firmy jak i osoby prywatne.
- Zadaniem symulatora będzie wytworzenie umiejętność budowania, obserwacji i likwidowania kreowanych zagrożeń i zastosowania ich w przyszłej pracy zawodowej.
- Zastosowane rozwiązania mają pozwolić na utworzenie programu nauczania w którym studenci będą mogli doświadczyć realnych zagrożeń w zamkniętym środowisku. Realizm symulowanych zagrożeń nie będzie odbiegał od rzeczywistych.
- Możliwości symulatora:
  - Prezentacja mechanizmu ataku phishing zawartości strony przez złośliwe oprogramowanie oraz ćwiczenia z umiejętności weryfikacji certyfikatów SSL. Umiejętności odnajdywania potencjalnych artefaktów świadczących o aktywności złośliwego oprogramowania.
  - Prezentacja podstawowych zagrożeń dotyczących malware, w tym utrata kontroli nad komputerem.
  - Prezentacja zagrożeń związanych z pharmingiem umożliwiająca pokazanie mechanizmu modyfikacji zawartości adresu www w celu przekierowania użytkownika na fałszywą stronę, mimo wpisania prawidłowego adresu strony.

NOWY WYMIAR STUDIOWANIA w WSPIA
PROJEKT „NOWY WYMIAR STUDIOWANIA W WSPIA”
PROJEKT WSPÓŁFINANSOWANY ZE ŚRODKÓW EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO
W RAMACH PROGRAMU OPERACYJNEGO WIEDZA EDUKACJA I ROZWÓJ 2014-2020
PROJEKT NR POWR.03.05.00-00-z045/17