**70/20** Załącznik nr 3 a

do §5 pkt. 1.2 Regulaminu gospodarowania środkami publicznymi

o wartości szacunkowej do 30 000 euro netto

**ISTOTNE WARUNKI ZAMÓWIENIA**

Procedura udzielenia zamówienia publicznego poniżej kwoty 30.000 euro netto

zgodnie z art. 4 pkt 8 Ustawy Prawo Zamówień Publicznych

1. Nazwa i adres ZAMAWIAJĄCEGO

Śląskie Centrum Chorób Serca w Zabrzu

Dział ………………………………….

ul. M. Curie-Skłodowskiej 9, 41-800 Zabrze

tel./fax. ……………………………….

1. Nazwa przedmiotu zamówienia

***OPROGRAMOWANIE DO MONITOROWANIA PODATNOŚCI***

1. Wymagania związane z wykonaniem:

Zgodnie z załącznikiem – załącznik nr 1

1. Oferta.

Ofertę należy złożyć na **Formularzu Oferty** (załącznik nr 1) w formie pisemnej w terminie do dnia **07/10/2020 r do godz. 9:00** w siedzibie Zamawiającego, tj. w budynku medyczno-administracyjnym „B” Śląskiego Centrum Chorób Serca w Zabrzu, mieszczącego się przy ul. M. Curie-Skłodowskiej 9, w Dziale Zaopatrzenia, Gospodarki Magazynowej i Transportu (pokój nr 2B3). lub drogą elektroniczną mailem na adres [mailowy s.jankowska@sccs.pl](mailto:mailowy%20s.jankowska@sccs.pl) [e.cybulska@sccs.pl](mailto:e.cybulska@sccs.pl) (skany) lub faxem na nr 32/278-43-35 **Formularz oferty** musi być wypełniony, podpisany i opieczętowany (pieczątką firmową i imienną) przez osobę/y uprawnioną/e do reprezentowania Wykonawcy.

* 1. Do oferty należy załączyć:
     + aktualny odpis z właściwego rejestrualbo aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej
     + zaakceptowane Istotne Warunki Zamówienia
     + ~~na wezwanie Zmawiającego próbki przedmiotu zamówienia~~
  2. Kryterium wyboru oferty: 100% cena/inne …………………..\* (niepotrzebne skreślić)

1. Tryb postępowania:

1. Zamawiający poinformuje Wykonawcę o przyjęciu lub nieprzyjęciu oferty w terminie do 30 dni od dnia upływu terminu składania ofert – zamieszczając wynik postępowania na stronie internetowej szpitala.

1. Zamawiający zastrzega sobie prawo zmiany terminu składania ofert lub zmiany warunków zamówienia.
2. Zamawiający zastrzega sobie prawo zakończenia postępowania bez wybrania żadnej ze złożonych ofert.
3. W razie nieprzyjęcia oferty Wykonawcy nie przysługują jakiekolwiek roszczenia w stosunku do Zamawiającego.

Zatwierdzam:

……………………………………

(podpis Kierownika Zamawiającego)

Pieczęć Wykonawcy

Załącznik nr 3 b

do §5 pkt. 1.2 Regulaminu gospodarowania środkami publicznymi

o wartości szacunkowej do 30 000 euro netto

**FORMULARZ OFERTY**

Część B (wypełnia Wykonawca)

I. Nazwa i adres WYKONAWCY:

……………………………………………………………………

……………………………………………………………………

……………………………………………………………………

nr telefonu ……………………………………………………….

NIP : ……………………………………………………………..

1. Nazwa przedmiotu zamówienia:

***OPROGRAMOWANIE DO MONITOROWANIA PODATNOŚCI***

1. Oferuję wykonanie przedmiotu zamówienia za kwotę:

* **Wartość netto ……………………………… zł**
* **Wartość brutto …………………………….. zł**
* **Podatek VAT …………. %, ……………… zł**

1. Deklaruję ponadto:
   1. Termin płatności: (min 30 dni) ……..…….dni
   2. ~~Okres gwarancji: ……………………..(min. 36 m-cy)~~
   3. Termin wykonania zamówienia 36 m cy
2. Oświadczam, że:

- akceptujemy projekt umowy\*/ istotne postanowienia umowy\* (*\*niepotrzebne skreślić)*

- po zapoznaniu się z opisem przedmiotu zamówienia nie wnosimy do niego zastrzeżeń,

- w razie wybrania naszej oferty zobowiązujemy się do realizacji zamówienia na warunkach określonych w Formularzu Oferty, w miejscu i terminie określonym przez Zamawiającego.

- termin związania z ofertą wynosi 30 dni

5. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:

…………………………………………………………………………..

…………………………………………………………………………

Data…………………………….. ………………………………

Podpis i pieczątka Wykonawcy

SCCS/06/2019

**PAKIET I**

***OPROGRAMOWANIE DO MONITOROWANIA PODATNOŚCI***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| l.p. | | | Nazwa przedmiotu zamówienia | | | | | j.m. | Ilość | Cena jedn. netto | Stawka VAT | Wartość brutto |  |  |  |  |  |  | Ilość | Cena jedn. netto | VAT | Wartość ogólna brutto |
| 1 | | | Oprogramowanie do monitorowania podatności | | | | | stanowisko | 50 |  |  |  |  |  |  |  | 2.500 |  |  |  |
|  | | | |  |  | |
|  |  |  | | | |

Wartość netto ………………………………………….

Wartość brutto …………………………………………..

………………………………………… podpis osoby upoważnionej

***OPIS PRZEDMIOTU ZAMÓWIENIA***

**Wymagania techniczne dla „Oprogramowania do monitorowania podatności”**

1. Rozwiązanie polega na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa
2. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
3. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
4. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:

* Microsoft Edge
* Mozilla Firefox
* Google Chrome
* Safari

1. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
2. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
3. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:

* Windows 2008 R2
* Windows 2012
* Windows 2012 R2
* Windows 2016
* Windows 2019

1. Portal zarządzający musi umożliwiać:

* przegląd wybranych danych na podstawie konfigurowalnych widgetów
* zablokowania możliwości zmiany konfiguracji widgetów
* zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
* tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
* eksport wszystkich skanów podatności do pliku CSV

1. Rozwiązanie musi umożliwiać uruchomienie skanu wykrywającego dostępne hosty w sieci
2. Skan wykrywający dostępne hosty w sieci musi umożliwiać:

* pracę w oparciu identyfikację hosta na podstawie protokołu ARP, ICMP PING, SSH, HTTP, HTTPS, RDP
* pracę w oparciu o analizę wszystkich dostępnych otwartych portów
* konfigurację zakresu skanowanych portów, wydajność skanu, liczbę wątków oraz możliwość wykrycia wersji systemu operacyjnego
* konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia
* konfigurację wysyłania powiadomień na wskazany adres e-mail w momencie rozpoczęcia skanu oraz jego zakończenia

1. Portal zarządzający musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu
2. Portal zarządzający musi umożliwiać eksport wyniku skanu wykrywającego dostępne hosty w sieci do pliku XLS oraz XML
3. Rozwiązanie musi umożliwiać uruchomienie skanu wykrywającego znane podatności
4. Skan wykrywający znane podatności musi umożliwiać:

* określenie skanowanego celu za pomocą adresu IP oraz podsieci IP
* konfigurację grupy skanów do której będzie przypisany
* masowe wprowadzenie skanowanych celów za pomocą pliku CSV
* konfigurację parametrów skanu (zakres portów TCP/UDP, parametr wydajności skanowania, rodzaj autentykacji) niezależnych od parametrów dziedziczonych z grupy skanów
* konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia
* konfigurację wysyłania powiadomień na wskazany adres e-mail w momencie rozpoczęcia skanu oraz jego zakończenia

1. Portal zarządzający musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających znane podatności wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu
2. Portal zarządzający musi umożliwiać eksport wyniku skanu wykrywającego znane podatności do pliku XLS oraz XML
3. Rozwiązanie musi umożliwiać uruchomienie skanu wykrywającego luki w aplikacjach webowych
4. Skan wykrywający luki w aplikacjach webowych musi umożliwiać:

* określenie skanowanego celu za pomocą adresu URL
* konfigurację grupy skanów do której będzie przypisany
* konfigurację parametrów skanu (rodzaje ataków, wyjątki ze skanowania, nagłówki, parametr wydajności skanowania) niezależnych od parametrów dziedziczonych z grupy skanów
* konfigurację rodzaju nagrywania sesji podczas przeprowadzanego skanu
* konfigurację rodzaju autentykacji (HTTP/Form)
* konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia
* konfigurację wysyłania powiadomień na wskazany adres e-mail w momencie rozpoczęcia skanu oraz jego zakończenia

1. Portal zarządzający musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu
2. Portal zarządzający musi umożliwiać eksport wyniku skanu wykrywającego luki w aplikacjach webowych do pliku XLS oraz XML
3. Rozwiązanie musi umożliwiać wykorzystanie narzędzia do identyfikacji adresów internetowych
4. Narzędzie do identyfikacji adresów internetowych musi umożliwiać:

* wyszukiwanie adresów internetowych spełniających wskazane warunki
* zapisywanie wskazanych warunków wyszukiwania jako szablony
* podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych
* dodanie wybranych wyników wyszukiwania do grupy skanów podatności

1. Rozwiązanie musi umożliwiać podgląd listy wszystkich wykrytych podatności z wszystkich skanów
2. Lista wszystkich wykrytych podatności musi umożliwiać:

* filtrowanie podatności ze względu na ich rodzaj, przypisany tag, host na którym została znaleziona, stopień zagrożenia, status
* wyświetlenie szczegółów poszczególnych podatności wraz z informacjami na jakich hostach została wykryta
* eksport listy hostów na których została wykryta dana podatność do pliku CSV

1. Rozwiązanie musi umożliwiać podgląd listy wygenerowanych raportów
2. Rozwiązanie musi umożliwiać utworzenie nowego raportu podsumowującego:
3. Raport podsumowujący musi umożliwiać:

* konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu
* wybranie grup skanów, które będą znajdowały się w raporcie
* wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie
* określenie danych klienta, którymi zostanie podpisany raport

1. Lista wygenerowanych raportów musi umożliwiać:

* filtrowanie raportów ze względu na ich autora, nazwę, szablon oraz opis
* eksport wyniku raportu do pliku CSV, DOC, XLS

1. Rozwiązanie musi umożliwiać:

* podgląd listy utworzonych zgłoszeń
* filtrowanie zgłoszeń ze względu na ich status oraz czas zamknięcia
* podgląd listy szablonów dla poszczególnych rodzajów skanów
* dodanie szablonu dla poszczególnych rodzajów skanów oraz wprowadzenie ich konfiguracji
* zarządzanie listą użytkowników oraz przypisywanie ich do grupy
* konfigurację grup użytkowników z odpowiednimi uprawnieniami do poszczególnych grup skanów
* wprowadzenie restrykcji adresu IP z którego następuje logowanie
* wymuszenie weryfikacji dwuetapowej podczas logowania
* podgląd wszystkich zdarzeń w systemie uwzględniając użytkownika, adres IP oraz rodzaj zdarzenia
* wykorzystanie API do integracji danych z innymi środowiskami

**70/20 ZU**

**PROJEKT UMOWA NR / /EZ/2020**

zawarta w dniu………………pomiędzy:

**ŚLĄSKIM CENTRUM CHORÓB SERCA W ZABRZU,**

Samodzielnym publicznym zakładem opieki zdrowotnej z siedzibą: 41-800 Zabrze, ul. M.C. Skłodowskiej 9, zarejestrowanym w Krajowym Rejestrze Sądowym w Sadzie Rejonowym w Gliwicach Wydział X Gospodarczy KRS pod nr 0000048349, NIP 6482302807, zwanym dalej **„Zamawiającym”** reprezentowanym przez

Bożena Duda – Dyrektor ds. ekonomiczno - administracyjnych   
oraz firmą

…………………………………………………………………………………………………………………………………………………………………………………………………… reprezentowanym przez ……………………………………………………………., zwanym w dalszej treści umowy **„Wykonawcą”**.

**§ 1**

Zamawiający zamawia, a Wykonawca przyjmuje do wykonania dostawę licencji na oprogramowanie do monitorowania podatności dla 50 stacji roboczych z trzyletnim wsparciem serwisowym zgodnie ze złożoną ofertą i zapytaniem ofertowym stanowiącymi integralną część umowy.

**§ 2**

1. Wykonawca zobowiązuje się do dostarczenia przedmiotu zamówienia określonego w § 1, w terminie **do 14 dni od dnia zawarcia umowy**.
2. Zamawiający w terminie do 2 dni roboczych od dostarczenia potwierdzi drogą elektroniczną odbiór przedmiotu umowy bez zastrzeżeń.
3. Wykonawca oświadcza, że posiada zgodę producenta oprogramowania, o którym mowa w § 1, na dostarczenie licencji końcowemu użytkownikowi w załączniku do umowy nr 1.

**§ 3**

1. Zamawiający zobowiązuje się wypłacić Wykonawcy wynagrodzenie w kwocie:

– **netto ....................... zł** (słownie: ......................................... ),

– **brutto ....................... zł** (słownie: ......................................... ).

1. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego poleceniem przelewu na rachunek bankowy Wykonawcy.

**§ 4**

1. Zamawiający zapłaci Wykonawcy za przedmiot umowy, po odbiorze bez zastrzeżeń oraz wystawieniu faktury VAT, w terminie 30 dni. W przypadku zastrzeżeń przy odbiorze przedmiotu umowy faktura nie zostanie zrealizowana.
2. Zamawiający oświadcza, że jest płatnikiem podatku VAT i upoważnia Wykonawcę   
   do wystawienia faktury bez podpisu Zamawiającego.
3. Zamawiający upoważnia Wykonawcę do przesłania faktur elektronicznych na adres email Zamawiającego: …………………………...

**§ 5**

1. Wykonawca zapłaci Zamawiającemu kary umowne w przypadku:
2. nie przystąpienia do wykonania zamówienia, niewykonania lub nienależytego wykonania zamówienia, odstąpienia od umowy przez Wykonawcę, bądź przez Zamawiającego, z przyczyn za które odpowiedzialność ponosi Wykonawca,   
   w wysokości 10% wynagrodzenia brutto określonego w § 3 ust. 1 niniejszej umowy,
3. zwłoki w wykonaniu przedmiotu umowy, w wysokości 0,5 % wynagrodzenia brutto określonego w § 3 ust. 1 niniejszej umowy, za każdy dzień zwłoki, liczony od terminów określonych w § 2 ust. 1.
4. Jeżeli kary umowne nie pokrywają poniesionej szkody Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach określonych w Kodeksie Cywilnym.
5. Zamawiający może potrącić kary umowne, o których mowa w ust. 1 z wynagrodzenia Wykonawcy bez uprzedniego wezwania do ich zapłacenia.
6. Kary umowne mogą być naliczane łącznie i podlegają kumulacji.
7. Zamawiający w terminie 7 dni ma prawo odstąpić od umowy w przypadku zwłoki  
   w wykonaniu przez Wykonawcę przedmiotu umowy wynoszącej więcej niż 2 dni roboczych licząc od terminu wskazanego w § 2 ust. 1.

**§ 6**

Strony uzgadniają, że nie będą naliczać kar umownych za nieterminową realizację umowy wynikłą z przyczyn tzw. siły wyższej tj. powodzie, klęski żywiołowe, wprowadzenie stanu wyjątkowego, katastrofy dotyczące stron i mające wpływ na wykonanie przedmiotu umowy. W takich przypadkach strona dotknięta skutkami działania siły wyższej zobowiązana jest   
do niezwłocznego poinformowania drugiej strony, po czym strony przeprowadzą negocjacje w celu wypracowania metod dalszego wspólnego postępowania.

**§ 7**

1. W kwestiach nie uregulowanych w niniejszej umowie mają zastosowanie odpowiednie przepisy Kodeksu Cywilnego oraz innych obowiązujących w tym zakresie przepisów prawa.
2. Wszelkie zmiany w niniejszej umowie wymagają formy pisemnej pod rygorem nieważności.
3. Wszelkie ewentualne spory wynikłe na tle realizacji umowy Strony będą rozstrzygać ugodowo. W razie braku szans zawarcia ugody, właściwym do rozstrzygnięcia sporu Strony ustalają sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.

**§ 8**

Umowę niniejszą sporządzono w 2 jednobrzmiących egzemplarzach, po jednym dla każdej ze stron

**ZAMAWIAJĄCY WYKONAWCA**

Załącznik do Umowy nr 1

**Warunki licencji** **oprogramowania do monitorowania podatności**