**ZAPYTANIE OFERTOWE**

**(na podstawie art. 28 ustawy Prawo zamówień publicznych
 – tj. z dnia 14 lipca 2023 r.**[**(Dz.U. z 2023 r. poz. 1605)**](https://sip.legalis.pl/document-view.seam?documentId=mfrxilrtg4ytsmrzgq4dm)

W celu zbadania oferty rynkowej oraz oszacowania wartości zamówienia,

**Zamawiający:**

**Ministerstwo Edukacji Narodowej**

**Al. Jana Chrystiana Szucha 25,**

**00-918 Warszawa**

Osoba upoważniona do kontaktów: Maciej Wilczyński

maciej.wilczynski@men.gov.pl tel. **+48 22 3474889**

zwraca się z prośbą o przedstawienie informacji dotyczących szacunkowych kosztów realizacji poniższego zamówienia.

1. **Opis przedmiotu zamówienia:**

Przedmiotem zamówienia jest dostawa, wdrożenie oraz utrzymanie zautomatyzowanej platformy do zaawansowanych testów penetracyjnych w infrastrukturze Zamawiającego.

Platforma zautomatyzowanych testów penetracyjnych powinna być w stanie objąć testami 1000 stacji roboczych oraz serwerów wskazanych przez Zamawiającego i znajdujących się w jego infrastrukturze IT. W ramach przedmiotu zamówienia, Wykonawca dostarcza Zamawiającemu 1000 licencji, ważnych przez 12 miesięcy - w formie subskrypcji. Platforma musi objąć testami pozostałe elementy podłączone do sieci IP Zamawiającego. Rozwiązanie musi być uruchomione na infrastrukturze Zamawiającego. Wszystkie komponenty platformy muszą być zainstalowane lokalnie (on-prem) w infrastrukturze Zamawiającego.

**Zadania Wykonawcy**

W ramach usługi dostarczenia Platformy zautomatyzowanych testów penetracyjnych Zamawiający wymaga szkolenia stacjonarnego w siedzibie Zamawiającego dla grupy do 7 osób, zakresem obejmującego:

* Uzyskanie wiedzy niezbędnej do przeprowadzenia testów penetracyjnych z użyciem dostarczanej platformy.
* Nabycie umiejętności stosowania dostarczonych narzędzi przez Wykonawcę
* Wprowadzenie do dostarczonej platformy automatycznych testów penetracyjnych.
* Omówienie sposobu konfiguracji i zarządzania dostarczaną platformą.
* Omówienie możliwości dostarczanej platformy i rodzajów możliwych do wykonania testów.
* Szczegółowe omówienie raportowania dostępnego w dostarczanej platformie.
* Część praktyczna szkolenia powinna być przeprowadzona na wdrożonej platformie.
* Wystawienie Certyfikatu uczestnictwa i nabycia umiejętności po szkoleniu wraz ze wskazaniem tematyki szkolenia.

Wsparcie swoim zakresem musi obejmować co najmniej:

* Konsultacje dotyczące działania systemu.
* W ramach wsparcia Zamawiający wymaga usług konsultacji w zakresie czynności, związanych z eksploatacją w liczbie roboczogodzin niezbędnej do uruchomienia funkcjonalności oprogramowania. W ramach konsultacji możliwe jest zlecanie m.in takich prac jak.:
1. implementacja krytycznych poprawek systemu zalecanych przez producenta
2. aktualizacja systemu do nowych wersji zalecanych przez producenta,
3. jednorazowy przegląd systemu,
4. jednorazowe opracowanie dodatkowych procedur i instrukcji oraz ich aktualizacja,
5. przyjmowanie i obsługa zgłoszeń problemów: 24 godziny na dobę, 7 dni w tygodniu przyjmowanie zgłoszeń problemów oraz zgłaszanie problemów.
* Wsparcie w analizie raportów i danych dostarczanych przez Platformę, nie częściej niż raz w miesiącu.
* Ocena i rekomendacja działań mających na celu usuwanie zidentyfikowanych luk bezpieczeństwa, nie częściej niż raz w miesiącu.
* Wsparcie w zakresie analizy ryzyka identyfikowanych luk bezpieczeństwa
* i współpraca w zakresie planowania ich usuwania lub zabezpieczenia w innej warstwie systemowej.
* Współpraca w dziedzinie architektury referencyjnej i zmian w kluczowych dla bezpieczeństwa punktach węzłowych.

**Wymagane Środowisko sprzętowe i programowe**

Środowisko bazodanowe architektura klient-serwer,

Część serwerowa aplikacji powinna działać w jednym ze wskazanych systemów serwerowych Linux lub MS Windows.

1. **WYMAGANIA TECHNICZNE**
* Platforma musi zapewniać przeprowadzanie, automatycznych, cyklicznych i rzeczywistych testów penetracyjnych.
* Platforma musi umożliwiać wykonanie testów typu black box, grey box, oraz ataków ukierunkowanych według wcześniej określonego scenariusza i zdefiniowanych celów.
* Producent narzędzia musi zapewniać własne bezpieczne exploity/payloady używane w narzędziu.
* Platforma musi posiadać strukturę bezagentową.
* Platforma musi zapewniać możliwość skanu podatności konkretnych adresów lub puli adresów IP oraz możliwość wykluczenia adresów IP. Rozwiązanie musi umożliwiać dodanie dodatkowych adresów IP do działającego już testu typu BlackBox lub GrayBox.
* Platforma musi wizualizować pełną ścieżkę ataku za pomocą łatwo czytelnego diagramu z przedstawionymi konkretnymi operacjami wykonanymi przez narzędzie. Przedmiotowy przebieg ataku musi zawierać co najmniej informacje o wykorzystanej podatności, metodzie/metodach przełamania istniejących zabezpieczeń oraz szczegółach osiągniętego celu ataku. Operacje platformy muszą być mapowane do framework-a MITRE ATT & CK (Adversarial Tactics, Techniques, and Common Knowledge).
* Platforma musi mieć zaimplementowane mechanizmy łamania haseł, umożliwiające badanie siły haseł wykorzystywanych przez pracowników organizacji.
* Platforma musi umożliwiać wykonanie testu sprawdzającego poprawność konfiguracji systemu Active Directory z punktu widzenia bezpieczeństwa oraz musi wskazywać rozpoznane błędne elementy konfiguracji.
* Platforma musi umożliwiać automatyczną weryfikację skuteczności zainstalowanych na testowanych punktach końcowych rozwiązań AV/XDR przy wykorzystaniu różnego typu rozbrojonego kodu typu malware.
* Platforma musi umożliwiać sprawdzenie czy atakujący może uzyskać dostęp do zdefiniowanych plików bazując na ich nazwach i/lub zawartości.
* Platforma musi umożliwiać weryfikację pod kątem wykorzystywania przez urządzenia sieciowe domyślnych haseł dostępowych.
* Platforma musi wizualizować w dynamicznej formie i w czasie rzeczywistym postępy ataku na infrastrukturę.
* Platforma musi umożliwiać zdefiniowanie wybranych punktów końcowych, użytkowników, zakresów adresów IP jako krytyczne w celu zwiększenia rangi zagrożenia w przypadku, gdy wykonywany test zakończony zostanie sukcesem.
* Platforma musi umożliwiać operatorowi na wybór dopuszczalnych metod ataku na infrastrukturę. Decyzja o dopuszczeniu do realizacji określone techniki na określonym elemencie infrastruktury musi być możliwa do podjęcia na etapie definiowania testu oraz w czasie trwania testu.
* Platforma musi umożliwiać operatorowi wskazanie konkretnej adresacji w postaci pojedynczych adresów, podsieci czy danych pozyskanych z pliku CSV, które będą podlegały testom bezpieczeństwa.
* Platforma musi umożliwiać generowanie przejrzystego raportu po zakończonym teście. Raport musi wskazywać elementy infrastruktury, które zostały skompromitowane, podać uzyskane dane, w tym również pozyskane dane uwierzytelniające użytkowników oraz musi podać sposób w jaki udało się te dane pozyskać.
* Platforma musi umożliwiać zdefiniowanie harmonogramu automatycznego wykonywania testów.
* Platforma musi umożliwiać integrację z systemami SIEM oraz wysyłanie danych za pomocą formatów Syslog, LEEF, CEF.
* Platforma musi umożliwiać wysyłanie powiadomień drogą mailową.
* Platforma musi posiadać mechanizmy bezpieczeństwa uniemożliwiające dokonywania operacji modyfikacji danych na środowisku produkcyjnym np. blokowania kont użytkownikom, nadpisywania danych, manipulowania danymi.
* Platforma musi sugerować działania naprawcze w związku z wykrytą podatnością konkretnej maszyny.
* Platforma musi umożliwiać ustawienie poziomu zaawansowania testu w infrastrukturze podczas przeprowadzanego testu penetracyjnego.
* Platforma musi udostępniać pełny raport działań narzędzia w infrastrukturze.
* Platforma musi posiadać możliwość zdefiniowania maksymalnego czasu ataku.
* Platforma musi mieć możliwość uaktualnienia z zewnętrznego nośnika.
* Platforma musi udostępniać interfejsy API do wykonywania poszczególnych akcji.
* Wymagane funkcjonalności platformy muszą działać także gdy nie ma ona dostępu do sieci zewnętrznej
* Rozwiązanie musi umożliwiać wykonanie testu przez osobę nie dysponującą wiedzą z zakresu testów penetracyjnych dzięki automatyzacji testów, w ramach której rozwiązanie musi samo rozpoznawać jakie są możliwe ścieżki ataku na infrastrukturę. Sprawdzenie stanu bezpieczeństwa infrastruktury musi być możliwe wykorzystując wszystkie oferowane przez rozwiązanie techniki ataku włączone jednocześnie.
* Przeprowadzane testy penetracyjne nie mogą zakłócać pracy sieci Zamawiającego
* Niedopuszczalne jest zastosowanie jakichkolwiek technik lub oprogramowania, którego działanie może nieodwracalnie uszkodzić jakiekolwiek elementy infrastruktury lub oprogramowania Zamawiającego.
* Wszystkie oczekiwane funkcjonalności muszą być realizowane przez oprogramowanie pochodzące od jednego dostawcy.
* Platforma musi umożliwiać wykonanie testów mających na celu zweryfikowanie odporności stacji końcowych oraz skuteczności uruchomionych na nich mechanizmów bezpieczeństwa w przypadku ataku typu Ransomware.
* Platforma musi umożliwiać wykonanie symulacji ataku poprzez emulację działania Ransomware na stacjach końcowych. Emulacja musi być w pełni bezpieczna, szyfrowanie musi być wykonane na kopi plików. Oryginalne pliki znajdujące się na objętej testami stacji nie mogą brać udziału w procesie szyfrowania.
* Platforma musi być w stanie wykonać w pełni bezpieczną emulację bazując co najmniej na Ransomware Maze i REvil.
* Platforma do wykonania testu typu Ransomware musi wykorzystywać konto użytkownika uprzywilejowanego tak aby umożliwić wykonanie testów w sposób bezagentowy.
1. **Warunki udziału w postępowaniu (np. szczególne uprawnienia, wymagana wiedza
i doświadczenie, warunki odnoszące się do norm zarządzania środowiskiem).**

W postępowaniu mogą wziąć udział oferenci, którzy spełniają następujące warunki:

1. posiadają odpowiednią wiedzę, doświadczenie oraz zasoby techniczne i kadrowe umożliwiające realizację przedmiotu zamówienia,
2. posiadają prawo do udzielania licencji na System, jego kody źródłowe oraz wszelką dokumentację.

W związku z wejściem w życie przepisów ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (zwana dalej „ustawą”), Zamawiający będzie badał czy nie zachodzą wobec Wykonawcy przesłanki wykluczenia, o których mowa w art. 7 ust. 1 ustawy. W przypadku zaistnienia przesłanek, o których mowa powyżej, oferta Wykonawcy zostanie odrzucona.

1. **Wymagania dotyczące oferty.**
2. Informacje, jakie Wykonawca musi uwzględnić w ofercie:

Przy wycenie Wykonawca ma podać cenę za dostawę oraz uruchomieniesystemu w siedzibie Zamawiającego**.**

1. Ofertę w postaci wypełnionego formularza ofertowego należy przekazać drogą elektroniczną na adres e-mail: maciej.wilczynski@men.gov.pl **do 02.12.24, godz. 18:00.**
2. Zamawiający zastrzega sobie prawo do jednorazowego uzupełnienia dokumentów.

UWAGA!

Niniejsze szacowanie wartości zamówienia nie stanowi oferty w rozumieniu art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem ani zapytaniem o cenę w rozumieniu ustawy Prawo Zamówień Publicznych. Informacja ta ma na celu wyłącznie rozpoznanie rynku i uzyskanie wiedzy na temat kosztów przedłużenia licencji czasowej do oprogramowania, wsparcia producenta oraz przeniesienia oprogramowania do siedziby Zamawiającego.

Formularz oferty

**na realizację zamówienia pn.** „**dostawa, wdrożenie oraz utrzymanie zautomatyzowanej platformy do zaawansowanych testów penetracyjnych” Zamawiającego oraz udzielenie przez Wykonawcę niezbędnych, czasowych licencji”**

## DANE WYKONAWCY

|  |  |
| --- | --- |
| **Nazwa wykonawcy:** |  |
| **Adres siedziby wykonawcy:** |  |
| **Osoba do kontaktu:** | ……………………………………………………………*(Imię i nazwisko, adres e-mail, nr telefonu)* |

## DANE OFEROWANEGO PRODUKTU

|  |  |
| --- | --- |
| **Cena jednostkowa brutto za licencje** |  |

|  |  |
| --- | --- |
| **Cena oferty brutto w zł za realizację**  |  |

 ………………………………………… ………………………………………

 miejscowość, data podpis(y) osoby(ób) uprawnionych

 do reprezentowania Wykonawcy