

Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia.

- 1.1. Przedmiotem zamówienia jest **dostawa licencji do platformy Cyber Range** (dalej Platforma) rozumiana jako dostawa licencji umożliwiających Zamawiającemu dostęp do Platformy wraz gwarancją producenta, na zasadach określonych w OPZ.
- 1.2. Realizacja przedmiotu zamówienia polega na dostawie w terminie 5 Dni Roboczych licencji uprawniającej do 24 miesięcznego dostępu do Platformy Cyber Range.
- 1.3. W szczególności przedmiot zamówienia obejmuje:
 - 1.3.1. Dostawę niezbędnych licencji.
 - 1.3.2. Świadczenie gwarancji producenta przez okres 24 miesięcy od daty dostarczenia licencji.
- 1.4. Zamawiający może wymagać przeprowadzenia testów Proof of Concept wszystkich lub wybranych funkcjonalności na etapie wyboru ofert w celu weryfikacji zgodności z OPZ. Scenariusz testowy zostanie przygotowany przez Zamawiającego.
- 1.5. Wykonawca ma obowiązek wskazać nazwę producenta i model produktu, który oferuje, wraz z kartą katalogową/specyfikacją techniczną potwierdzającą zgodność z wymaganiami OPZ.

2. Udostępnienie Platformy.

- 2.1. Wykonawca zapewni działanie 30 kont dostępowych do Platformy dla wskazanych przez Zamawiającego specjalistów.
- 2.2. Dostęp do Platformy przyznany zostanie na 24 miesiące.

3. Wymagania minimalne dla platformy Cyber Range:

- 3.1. **Architektura Systemu.**
 - 3.1.1. Platforma powinna być udostępniona jako usługa typu SaaS (Software-as-a-Service) dostępna co najmniej przez przeglądarkę internetową.
 - 3.1.2. Usługa musi być dostępna za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w wersjach aktualnych na dzień składania oferty.
 - 3.1.3. Platforma musi być dostępna poprzez szyfrowany protokół TLS w wersji co najmniej 1.2.
- 3.2. **Wymagania odnośnie producenta**
 - 3.2.1. Producent Platformy musi posiadać ważną certyfikację ISO 27001 oraz być zgodny z GDPR/RODO.

- 3.2.2. Producent Platformy musi posiadać dedykowanego konsultanta technicznego (polsko języczny konsultant).
- 3.2.3. Producent Platformy musi zapewnić gwarancję na etapie wdrożenia rozwiązania. (j.polski) z UoP.
- 3.3. **Zarządzanie dostępem do Platformy.**
- 3.3.1. Platforma musi umożliwiać przyznanie indywidualnych kont dla każdego z użytkowników wymienionych w pkt. 2.1.
- 3.3.2. Platforma musi umożliwiać Zamawiającemu zarządzanie kontami użytkowników pozwalając na:
- 3.3.2.1. Utworzenie konta dla nowego użytkownika.
- 3.3.2.2. Usunięcie konta istniejącego użytkownika.
- 3.3.2.3. Możliwość przeniesienia konta ze starego na nowego pracownika.
- 3.3.3. Platforma musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Platformy.
- 3.3.4. Platforma musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem mechanizmu Single Sign-On (SSO).
- 3.4. **Obligatoryjne wymagania funkcjonalne.**
- 3.4.1. Platforma musi być dostępna w trybie 24h / 7 przez cały rok z SLA na poziomie 99,5 , za wyjątkiem zgłoszonej wcześniej niedostępności.
- 3.4.2. Baza danych platformy musi być identyczna dla wszystkich zakupionych kont.
- 3.4.3. Interfejs platformy musi wspierać natywnie takie języki jak:
- 3.4.3.1. Polski
- 3.4.3.2. Angielski
- 3.4.4. Materiały edukacyjne dostępne na platformie do realizacji scenariuszy muszą obejmować takie języki jak:
- 3.4.4.1. Polski
- 3.4.4.2. Angielski
- 3.4.5. Platforma musi posiadać moduł umożliwiający budowanie własnych środowisk testowych, z wykorzystaniem udostępnionych w systemie takich elementów jak:
- 3.4.5.1. Routery
- 3.4.5.2. Przetącniki
- 3.4.5.3. Firewalle
- 3.4.5.4. Maszyny wirtualne, z uwzględnieniem minimum:
- 3.4.5.4.1. Microsoft Windows 10
- 3.4.5.4.2. Microsoft Windows 11
- 3.4.5.4.3. Windows Server 2019
- 3.4.5.4.4. Windows Server 2022
- 3.4.5.4.5. Linux Debian 11
- 3.4.5.4.6. Linux Debian 12
- 3.4.5.4.7. Linux Ubuntu 22.04
- 3.4.5.4.8. Linux Ubuntu 24.04

- 3.4.6. Platforma musi zapewniać niezbędne licencje na korzystanie z oprogramowania do wykorzystywania maszyn wymienionych w pkt. 3.4.5.
- 3.4.7. Platforma musi umożliwiać ustawienie konkretnych parametrów maszyn zgodnie z potrzebami użytkownika, takie jak:
 - 3.4.7.1. Ilość vCPU
 - 3.4.7.2. Ilość RAM
- 3.4.8. Platforma musi graficznie przedstawiać połączenia pomiędzy poszczególnymi elementami wymienionymi w pkt. 3.4.4.
- 3.4.9. Platforma musi umożliwiać obsługę elementów wymienionych w pkt. 3.4.4. za pomocą konsoli oraz GUI.
- 3.4.10. Platforma powinna posiadać scenariusze zbudowane w oparciu o bazę MITRE ATT&CK.
- 3.4.11. Platforma powinna posiadać wbudowane narzędzie do analizy logów w podczas pracy przy scenariuszach.
- 3.4.12. Platforma powinna posiadać moduł CTF Capture the flag pozwalający na rywalizację pomiędzy uczestnikami zespołu.
- 3.4.13. Moduł CTF musi umożliwiać:
 - 3.4.13.1. Utworzenie zawodów w oparciu o z góry zaimplementowane przez Wykonawcę scenariusze w Cyber Range.
 - 3.4.13.2. Utworzenie zawodów z nowo zbudowanych własnych środowisk testowych.
 - 3.4.13.3. CTF musi umożliwiać zbieranie punktów za poszczególne etapy zawodów.
 - 3.4.13.4. CTF musi posiadać zestawienie podsumowujące uzyskane wyniki pomiędzy uczestnikami biorącymi udział w zawodach.
 - 3.4.13.5. CTF musi posiadać możliwość zdefiniowania konkretnego harmonogramu czasu kiedy następuje rozpoczęcie oraz koniec danych zawodów.
- 3.4.14. Platforma powinna posiadać wbudowane środowisko treningowe z dostarczonymi przez dostawcę różnego rodzaju ćwiczenia.
- 3.4.15. Ćwiczenia powinny poruszać kwestie ataków i zagrożeń na jakie nastawione są środowiska medyczne w tym w szczególności szpitale i placówki medyczne.
- 3.4.16. Platforma musi poruszać w ćwiczeniach w szczególności takie tematy jak:
 - 3.4.16.1. Tworzenie silnych haseł i analiza polityk
 - 3.4.16.2. Przedstawienie skutków kliknięcia w złośliwy link
 - 3.4.16.3. Rozpoznawanie fałszywych stron (phishing)
 - 3.4.16.4. Bezpieczne korzystanie z poczty elektronicznej
 - 3.4.16.5. Eksploatacja podatności:
 - 3.4.16.5.1. SQLi
 - 3.4.16.5.2. SSRF
 - 3.4.16.5.3. XSS
 - 3.4.16.5.4. CSRF
 - 3.4.16.6. Ataki phishingowe
 - 3.4.16.7. Ataki brute-force na loginy i hasła
 - 3.4.16.8. Privilege Escalation

- 3.4.16.9. Lateral movement i persistence w sieci
- 3.4.16.10. Reverse Engineering i komunikacja C2
- 3.4.16.11. Rekonesans usług z wykorzystaniem narzędzi
- 3.4.16.12. Ataki na Active Directory w szczególności Pass-the-Hash, Kerberoasting
- 3.4.16.13. Exploitacja zdanych serwisów
- 3.4.16.14. Detekcja i analiza logów
- 3.4.16.15. Praca z narzędziami SIEM
- 3.4.16.16. Monitorowanie ruchu sieciowego za pomocą narzędzi, np. Wireshark
- 3.4.16.17. Analiza plików i rejestru systemowego
- 3.4.16.18. Budowanie i analiza reguł Snort
- 3.4.16.19. Hardening systemów: OS, aplikacji
- 3.4.16.20. Analiza anomalii i wewnętrznego ruchu
- 3.4.16.21. Korelacja zdarzeń z różnych źródeł - SIEM
- 3.4.16.22. Wykrywanie phishingu z podejrzanym załącznikiem
- 3.4.16.23. Ataki ukierunkowane na rzuty pamięci, wykradanie danych, nadpisywanie wartości pamięci
- 3.4.16.24. Symulacja ataków na ICS/SCADA
- 3.4.16.25. Ataki na kontroler domeny
- 3.4.16.26. Wykrywanie podatności w Docker
- 3.4.16.27. Symulacja podatnych aplikacji w CI/CD - opcjonalne
- 3.4.16.28. Wykrywanie błędów w kodzie (Static Application Security Testing - SAST) - opcjonalne
- 3.4.17. Platforma powinna umożliwiać filtrowanie poszczególnych ćwiczeń w oparciu o ich:
 - 3.4.17.1. Tematykę w odniesieniu do pkt. 3.4.13.
 - 3.4.17.2. Poziom trudności
 - 3.4.17.2.1. Łatwe
 - 3.4.17.2.2. Średnie
 - 3.4.17.2.3. Trudne
 - 3.4.17.3. Przeznaczenie dla określonej grupy pracowników, np:
 - 3.4.17.3.1. Red Team
 - 3.4.17.3.2. Blue Team
 - 3.4.17.3.3. Security Analyst
 - 3.4.17.3.4. Forensic Analyst
 - 3.4.17.3.5. Incident Responder
 - 3.4.17.3.6. Penetration Tester
- 3.4.18. Platforma musi poruszać w laboratoriach tematykę i sposoby aktualnie wykorzystywanych w świecie podatności CVE.
- 3.4.19. Platforma musi poruszać w laboratoriach tematykę i sposoby aktualnie wykorzystywanych w świecie trendów w zakresie podatności oprogramowania.
- 3.4.20. Platforma musi poruszać w laboratoriach tematykę i sposoby aktualnie wykorzystywanych w świecie ataków typu ransomware.
- 3.4.21. Platforma musi umożliwić użytkownikowi:

- 3.4.21.1. Rozpoczęcie ćwiczenia
- 3.4.21.2. Wstrzymanie ćwiczenia wraz z zastopowaniem czasu jego wykonywania
- 3.4.21.3. Wznowienie danego wstrzymanego ćwiczenia
- 3.4.22. Platforma musi posiadać zestawienie podsumowujące osiągnięcia danego uczestnika obejmujące uzyskane wyniki w środowisku treningowym.
- 3.4.23. Niedopuszczalne jest rozdzielenie obsługi na więcej niż jeden portal.

3.5. Gwarancja

- 3.5.1. Licencje muszą być dostarczone wraz z gwarancją producenta.
- 3.5.2. Możliwość udziału w bezpłatnych warsztatach i szkoleniach z obsługi Platformy organizowanych przez producenta oprogramowania.
- 3.5.3. Gwarancja musi być dostępna w trybie 24 / 7 z możliwością zgłaszania problemów za pomocą telefonu, wiadomości e-mail lub dedykowanego portalu www.
- 3.5.4. Możliwość skorzystania bezpłatnie z konsultacji z producentem oprogramowania.
- 3.5.5. Dostępność bazy wiedzy, opisującej szczegóły konfiguracji Platformy oraz dobrych praktyk w zakresie Cyber Range.
- 3.5.6. Gwarancja musi zapewniać dostęp do materiałów szkoleniowych producenta.
- 3.5.7. W ramach gwarancji wymaga się od konsultanta wsparcia w zakresie definicji i wdrożenia przypadków użycia oraz architektury rozwiązania.

3.6. Instruktaż stanowiskowy

Przeprowadzenie instruktażu dla nie więcej niż 20 wskazanych przez Zamawiającego pracowników w języku polskim.
Instruktaż przygotuje wskazanych pracowników do samodzielnego wykorzystania Platformy.
Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

- 3.6.1. Instruktaż zostanie zorganizowany w czasie ustalonym z Zamawiającym po podpisaniu umowy.
- 3.6.2. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego, zdalnie lub w ustalonej sali szkoleniowej za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.
- 3.6.3. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:
 - 3.6.3.1. Architektura produktu.
 - 3.6.3.2. Poruszanie się po interfejsie użytkownika.
 - 3.6.3.3. Planowanie wdrożenia systemu wraz z architekturą systemu.
 - 3.6.3.4. Instalacja konsoli zarządzania i agentów na stacjach końcowych.
 - 3.6.3.5. Wykonanie przykładowych scenariuszy.
 - 3.6.3.6. Zaprezentowanie możliwości działania CTF.
 - 3.6.3.7. Zaprezentowanie możliwości tworzenia nowych środowisk testowych.
 - 3.6.3.8. Wyszukiwanie zaawansowane w platformie.
 - 3.6.3.9. Konfiguracja dashboardów.