**Załącznik nr 4 do SWZ– OPZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest dostawa subskrypcji **Systemu Ochrony Ruchu DNS**, zwanego dalej **SOR DNS**, dostawa licencji na Oprogramowanie wraz z Usługą Wdrożenia oraz Usługą Utrzymania i Wsparcia Technicznego. System Ochrony Ruchu DNS będzie wykorzystywany do ochrony ruchu DNS w ramach całej Sieci Badawczej Łukasiewicz, tj. w Centrum Łukasiewicz (Zamawiający) oraz   
w Instytutach wchodzących w skład Sieci Badawczej Łukasiewicz, zwanej dalej SBŁ. SBŁ użytkuje obecnie system SOR DNS oparty na rozwiązaniu BloxOneTreat Defense Business Cloud, z subskrypcją oraz licencjami obowiązującymi do 11 grudnia 2024 roku.

1. Wymagania ogólne
   1. Cele główne systemu SOR DNS w SBŁ

Wykorzystanie ruchu w protokole DNS jest popularną metodą przeprowadzania ataków malware (w tym ransomware), doprowadzania do wycieków danych oraz korzystania   
z tylnych furtek cyberprzestępców (backdoor). Zamawiany system SOR DNS ma za zadanie pełnić rolę usługi DNS dla urządzeń SBŁ, a także analizować ruch w protokole DNS   
i wykrywać wszystkie niepożądane zdarzenia, aby:

* + 1. Zapewniać ochronę zasobów sieci IT SBŁ przed wyciekiem danych przez protokół DNS;
    2. Zapewniać ochronę zasobów sieci IT SBŁ przed zagrożeniami typu Advanced Persistent Threat (APT) i zero-day wykorzystującymi ruch DNS;
    3. Zapewniać ochronę serwerów DNS SBŁ przed atakami typu DDoS;
    4. Zapewniać kontrolę dostępu aplikacji i użytkowników do stron www (filtering).

* 1. Wymagania dotyczące subskrypcji

Dostarczona subskrypcja musi umożliwiać legalne korzystanie z funkcji SOR DNS opisanych w dalszej części OPZ przez użytkowników, którymi będą pracownicy SBŁ. Subskrypcja pozwoli na wykorzystanie SOR DNS w działalności gospodarczej i naukowej, co najmniej na terenie Polski:

* + 1. Subskrypcja musi zapewniać ochronę ruchu DNS przez SOR DNS i wykorzystanie opisanych w OPZ funkcjonalności dla 6010 użytkowników:
    - w przypadku zawarcia Umowy przed 12 grudnia 2024 r. przez okres 12 miesięcy od dnia 12 grudnia 2024 r.;
    - w przypadku zawarcia Umowy po 12 grudnia 2024 r. przez okres 12 miesięcy od dnia prawidłowej dostawy subskrypcji oraz licencji potwierdzonej protokolarnie;
    1. W ramach subskrypcji Zamawiający musi mieć możliwość instalowania i użytkowania oprogramowania serwerów SOR DNS Proxy (patrz punkt I.3.b. Dostęp do usługi SOR DNS Cloud (patrz punkt I.3.a) nie może być ograniczony ze względu na liczbę serwerów SOR DNS Proxy. Musi być możliwa instalacja wielu serwerów SOR DNS Proxy w jednej lub wielu lokalizacjach w SBŁ.
    2. W ramach subskrypcji Zamawiający musi mieć możliwość instalowania i użytkowania oprogramowania agentów SOR DNS Agent (patrz punkt I.3.c). Dostęp do usługi SOR DNS Cloud (patrz punkt I.3.a) nie może być ograniczony ze względu na liczbę agentów SOR DNS Agent. Zamawiający musi mieć możliwość instalacji agentów SOR DNS Agent na wszystkich urządzeniach mobilnych i stacjach klienckich, z których korzystają użytkownicy SBŁ.
    3. W ramach subskrypcji użytkownicy SBŁ muszą mieć możliwość wykonania w okresie jej trwania co najmniej 32 000 zapytań dotyczących reputacji domeny / adresu IP do każdego źródła danych, o którym mowa w punkcie VI.1.
    4. W ramach subskrypcji Wykonawca zapewni Wsparcie Techniczne producenta SOR DNS, w ramach którego producent będzie dostarczał Aktualizacje systemu SOR DNS, a także uaktualniał: listy zagrożeń, kategorie treści oraz sygnatury i mechanizmy silnika analitycznego SOR DNS Cloud.
  1. Architektura i komponenty SOR DNS

**System SOR DNS** musi składać się z następujących komponentów:

* + 1. Zewnętrzna usługa chmurowa chronionego ruchu DNS o wysokiej dostępności, zwana dalej **SOR DNS Cloud** (patrz punkt II.).
    2. Serwery proxy DNS instalowane w sieci wewnętrznej SBŁ, zwane dalej **SOR DNS Proxy** (patrz punkt III.).
    3. Oprogramowanie instalowane na urządzeniach SBŁ, w tym w szczególności na stacjach klienckich i urządzeniach mobilnych, zwane dalej **SOR DNS Agent** (patrz punkt IV.).
    4. Powyższa architektura musi:
       1. być integralna, co oznacza, że jej komponenty współpracują ze sobą, aby realizować cele główne SOR DNS;
       2. zapewniać skalowalność i dopasowanie do architektury SBŁ, rozumiane jako możliwość instalacji wielu serwerów SOR DNS Proxy w jednej lub wielu lokalizacjach SBŁ, jak również funkcjonowanie SOR DNS Agent na stacjach i urządzeniach mobilnych także poza siecią wewnętrzną, bez konieczności dostępu sieciowego do SOR DNS Proxy.

1. Wymagania dotyczące SOR DNS Cloud
   1. SOR DNS Cloud musi udostępniać funkcjonalność przyjmowania i rekursywnego rozwiązywania zapytań DNS dla domen internetowych kierowanych bezpośrednio na jej publiczny internetowy adres IP, zgodnie z RFC 1035, dodatkowo z możliwością ograniczenia zakresu akceptowanych adresów źródłowych zapytań.
   2. SOR DNS Cloud musi udostępniać funkcjonalność przyjmowania i rekursywnego rozwiązywania zapytań DNS dla domen internetowych pośrednio, poprzez wirtualne serwery SOR DNS Proxy zainstalowane w sieci wewnętrznej IT SBŁ.
   3. SOR DNS Cloud musi udostępniać funkcjonalność przyjmowania i rekursywnego rozwiązywania zapytań DNS dla domen internetowych pośrednio poprzez SOR DNS Agent zainstalowany na stacjach roboczych i urządzeniach mobilnych.
   4. Ruch sieciowy pomiędzy SOR DNS Cloud, a SOR DNS Proxy musi być zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.
   5. Ruch sieciowy pomiędzy SOR DNS Cloud, a SOR DNS Agent musi być zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.
   6. SOR DNS Cloud musi wspierać walidację DNSSEC dla ruchu SOR DNS Proxy, SOR DNS Agent, a także dla zapytań bezpośrednich DNS.
   7. Konfiguracja SOR DNS Cloud musi być możliwa poprzez dostępny przez Internet portal www. Ruch sieciowy z portalem www musi być szyfrowany protokołem TLS, a dostęp do konfiguracji musi być ograniczony tylko dla uwierzytelnionych i zautoryzowanych użytkowników, przy czym musi być możliwe uwierzytelnienie zarówno jednoskładnikowe, jak i wieloskładnikowe.
   8. SOR DNS Cloud musi mieć możliwość zdefiniowania listy domen wewnętrznych przez autoryzowanych użytkowników, czyli takich dla których SOR DNS Proxy lub oprogramowanie SOR DNS Agent nie będzie przesyłać zapytań DNS do SOR DNS Cloud, ale zamiast tego prześle je do określonego wewnętrznego serwera DNS w sieci SBŁ.
   9. SOR DNS Cloud musi mieć możliwość automatycznego podejmowania działań   
      w odniesieniu do treści zapytań i odpowiedzi DNS, na podstawie zdefiniowanych przez autoryzowanych użytkowników polityk bezpieczeństwa, zgodnie z wymaganiami określonymi w punkcie V.
2. Wymagania dotyczące SOR DNS Proxy
   1. Ruch pomiędzy SOR DNS Proxy i SOR DNS Cloud musi być szyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS;
   2. SOR DNS Proxy musi dodawać do standardowych zapytań DNS informacje potrzebne SOR DNS Cloud do realizacji funkcji ochrony i funkcji gromadzenia danych analitycznych, w szczególności informacje o wew. prywatnym adresie IP komputera oraz o adresie MAC komputera;
   3. SOR DNS Proxy musi wspierać walidację DNSSEC dla ruchu w komunikacji z SOR DNS Cloud;
   4. SOR DNS Proxy musi mieć możliwość implementacji na maszynie wirtualnej VMware lub kontenerach Docker;
   5. SOR DNS Proxy musi integrować się z serwerami wewnętrznymi DNS w sieci SBŁ, korzystając z list o których mowa w II.8 i realizując zapytania o domeny wewnętrzne do tych serwerów;
   6. SOR DNS Proxy musi wspierać mechanizm Failover, dzięki którem w przypadku awarii SOR DNS Cloud, zostanie zachowana ciągłość działania usługi DNS w SBŁ dla urządzeń, które podlegały ochronie SOR DNS;
   7. SOR DNS Proxy musi umożliwiać konfigurację mechanizmu Anycast, dzięki któremu pod jednym adresem IP będzie możliwość połączenia ze zdefiniowaną grupą SOR DNS Proxy, w szczególności, w przypadku awarii części SOR DNS Proxy pozostałe serwery przejmą obsługę usługi DNS.
3. Wymagania dotyczące SOR DNS Agent
   1. Ruch pomiędzy SOR DNS Agent i SOR DNS Cloud musi być szyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS;
   2. SOR DNS Agent musi dodawać do standardowych zapytań DNS informacje potrzebne SOR DNS Cloud do realizacji funkcji ochrony i funkcji gromadzenia danych analitycznych, w szczególności informacje o wew. prywatnym adresie IP komputera oraz o adresie MAC komputera;
   3. SOR DNS Agent musi wspierać walidację DNSSEC dla ruchu w komunikacji z SOR DNS Cloud;
   4. SOR DNS Agent musi integrować się z serwerami wewnętrznymi DNS w sieci SBŁ, korzystając z list, o których mowa w II.8 i realizując zapytania o domeny wewnętrzne do tych serwerów;
   5. SOR DNS Agent musi działać na urządzeniach z systemami operacyjnymi:
      * MS Windows od wersji 10,
      * Mac OS od wersji 12,
      * Android od wersji 11,
      * IPhone IOS od wersji 14.
   6. SOR DNS Agent musi wspierać możliwość hurtowej instalacji w środowisku Active Directory przy wykorzystaniu mechanizmu GPO oraz w środowisku Apple z wykorzystaniem Apple Remote Desktop. Instalacja na urządzeniach mobilnych odbywać się musi poprzez system MDM lub standalone.
4. Wymagania dotyczące ochrony ruchu DNS
   1. SOR DNS Cloud musi mieć możliwość automatycznego podejmowania działań   
      w odniesieniu do zapytań i odpowiedzi DNS, na podstawie zdefiniowanych przez autoryzowanych użytkowników polityk bezpieczeństwa. Możliwe działania powinny obejmować:
      1. zezwolenie na zapytanie bez logowania,
      2. zezwolenie na zapytanie z jego odnotowaniem w logach,
      3. blokowanie zapytania przy pomocy odpowiedzi NXDomain (brak takiej domeny),
      4. przekierowanie (odpowiedź ze zdefiniowanym przez autoryzowanego użytkownika adresem IP, odpowiedź ze zdefiniowanym przez Zamawiającego adresem CNAME). Przekierowanie powinno być również możliwe do strony internetowej udostępnionej przez dostawcę z możliwością jej personalizacji przez autoryzowanego użytkownika.
   2. SOR DNS Cloud musi podejmować automatyczne działania na podstawie analizy ruchu DNS w kontekście zdefiniowanych i konfigurowanych przez autoryzowanych użytkowników polityk bezpieczeństwa. Polityki bezpieczeństwa będą definiować działania automatyczne   
      w oparciu o:
      1. listy zagrożeń (patrz V.3 do V.6),
      2. kategorie treści (patrz V.7),
      3. zagrożenia wykrywane na podstawie analizy ruchu przez silnik analityczny SOR DNS Cloud (patrz V.8).
   3. Mechanizmy polityk bezpieczeństwa oparte o listy zagrożeń będą funkcjonować w oparciu o listy:
      1. listy dostarczane przez producenta systemu SOR DNS,
      2. listy własne zarządzane przez autoryzowanych użytkowników.

Mechanizmy polityk bezpieczeństwa oparte o listy zagrożeń, będą analizować listy zagrożeń zawierające listy niebezpiecznych domen i adresów IP, pod kątem nazwy domeny w zapytaniu, nazwy domeny występującej jako CNAME dla nazwy z zapytania i na podstawie adresu IP w odpowiedzi. Działanie na podstawie nazw domen powinno funkcjonować dla dowolnego typu zapytania – system SOR DNS nie może pozwolić na ominięcie blokowania domeny przez wysyłanie określonych typów zapytań, takich jak SOA, MX lub NS.

* 1. Listy zagrożeń dostarczanych przez producenta systemu SOR DNS będą uaktualniane na bieżąco i muszą obejmować następujące listy:
     1. lista domen internetowych związanych z atakami APT,
     2. lista domen i adresów IP powiązanych ze złośliwym oprogramowaniem,
     3. lista domen związanych z ransomware,
     4. lista nazw i adresów IP publicznych serwerów DNS over HTTPS,
     5. lista domen powiązanych ze złośliwym oprogramowaniem korzystającym z algorytmów generowania domen (DGA),
     6. lista adresów IP węzłów wyjściowych sieci TOR,
     7. lista domen związanych z phishingiem,
     8. lista domen związanych z nieautoryzowanym generowaniem kryptowalut.
  2. Listy zagrożeń dostarczane przez producenta systemu SOR DNS muszą posiadać dane o zagrożeniach celujących w Polskę – co najmniej 66% domen z listy CERT.PL z ostatniego miesiąca musi znajdować się na listach z pkt V.4.
  3. SOR DNS Cloud musi umożliwiać autoryzowanym użytkownikom zdefiniowanie własnej listy niebezpiecznych domen / adresów IP i użycia ich w konfiguracji polityk bezpieczeństwa, na podstawie których SOR DNS Cloud ma podejmować reakcję. W przypadku list własnych zarządzanych przez autoryzowanych użytkowników, system SOR DNS musi mieć możliwość zdefiniowania poziomu zagrożenia i pewności informacji oddzielnie dla każdej listy. System SOR DNS musi umożliwiać tworzenie i edycję własnych list manualnie z portalu www klienta, automatycznie poprzez import z pliku CSV oraz poprzez interfejs API, aby umożliwić łatwy import zewnętrznych danych o zagrożeniach. System SOR DNS musi umożliwiać utworzenie min. 100 list własnych, łącznie o pojemności min. 500 000 rekordów.
  4. SOR DNS Cloud musi umożliwiać autoryzowanym użytkownikom definiowanie polityk bezpieczeństwa w oparciu o kategorie treści dla domen tak, aby SOR DNS Cloud podejmowała automatyczne działania w przypadku domen hostujących treści takie jak: pornografia, hazard, sieci społecznościowe, anonimizatory, reklamy itp. SOR DNS Cloud musi mieć aktualne informacje o kategorii treści dla domen.
  5. SOR DNS Cloud musi umożliwiać autoryzowanym użytkownikom definiowanie polityk bezpieczeństwa w oparciu o zagrożenia wykrywane na podstawie analizy ruchu przez silnik analityczny SOR DNS Cloud:
     1. SOR DNS Cloud musi mieć funkcję wykrywania i blokowania tunelowania DNS za pomocą silnika analitycznego opartego na uczeniu maszynowym i umożliwiającego wykrywanie nieznanych wzorców tunelowania i eksfiltracji danych przez DNS. System SOR DNS nie może działać wyłącznie w oparciu o sygnatury dla ruchu DNS znanych narzędzi tunelujących. System SOR DNS Cloud musi analizować co najmniej 10 atrybutów każdego zapytania DNS, które muszą obejmować: entropię znaków w FQDN, popularność w językach naturalnych wszystkich zestawów 2- i 3- znaków z nazwy FQDN, współczynnik występowania samogłosek w FQDN, współczynnik występowania cyfr   
        w FQDN, rozmiar zapytania, częstotliwość zapytań DNS (wartość częstotliwości i stałość częstotliwości).
     2. SOR DNS Cloud musi mieć funkcję wykrywania infiltracji przez DNS, w szczególności musi wykrywać technikę wykorzystywaną przez złośliwe oprogramowanie Powersource / DNS Messenger, to znaczy musi blokować próby przesyłania danych zakodowanych w odpowiedziach DNS w ramach rekordów TXT.
     3. SOR DNS Cloud musi mieć funkcję wykrywania nieznanych domen DGA i słownikowych DGA (domeny generowane z całych słów losowanych z 2-3 słowników) w zapytaniach DNS.
     4. SOR DNS Cloud musi mieć funkcję wykrywania domen fastflux.
  6. Kody do pomijania blokady:
     1. SOR DNS musi umożliwiać obejście blokowania domen/IP przy pomocy specjalnych kodów dostarczanych wybranym użytkownikom.
     2. SOR DNS musi umożliwiać wpisanie kodu na specjalnej stronie udostępnionej przez usługę SOR DNS Cloud, na którą następuje przekierowanie zgodnie z konfiguracją polityki bezpieczeństwa.
     3. Kody muszą mieć możliwość przypisania kategorii zagrożeń lub kategorii treści, których obejście umożliwiają.
     4. SOR DNS musi umożliwiać autoryzowanym użytkownikom generowanie kodów   
        do pomijania blokady.

1. Wymagania dotyczące funkcji analitycznych i raportowania
   1. Portal www usługi SOR DNS Cloud musi mieć funkcje pozwalające na analizę i reputacji domen, adresów IP, adresów URL. Dane o domenach/IP muszą pochodzić ze źródła producenta SOR DNS i co najmniej 2 innych dostawców danych. Narzędzie analityczne powinno bezpośrednio wyświetlać informacje o domenie / adresie IP co najmniej z bazy danych producenta SOR DNS o zagrożeniach opisanej w pkt. V.3 do V.5, z usługi pasywnego DNS, whois, rankingu popularności domen. Dostęp do narzędzia analizy będzie możliwy za pośrednictwem przeglądarki internetowej, a także poprzez interfejs API z danymi udostępnionymi w formacie JSON (do ich wykorzystania np. w narzędziach klasy SIEM).
   2. Portal www usługi SOR DNS musi zapewniać funkcje raportowania. Raporty powinny zawierać:
      1. Raporty aktywności pokazujące zapytania DNS wysłane do Usługi.
      2. Raporty bezpieczeństwa pokazujące zapytania DNS, dla których Usługa Chmurowa podjęła akcje zgodnie z polityką bezpieczeństwa.
      3. Raporty bezpieczeństwa muszą mieć możliwość filtrowania w oparciu o: źródło zapytania, adres oryginalnego źródła zapytania, adres MAC oryginalnego źródła zapytania, domena w zapytaniu, rodzaj w zapytaniu, odpowiedź, klasa zagrożenia (np. Malware), rodzaj zagrożenia (np. Malware C2), poziom zagrożenia, poziom zaufania do danych, nazwa użytkownika, podjęta akcja, lista zagrożeń, polityka bezpieczeństwa. Musi być również możliwość filtrowania w oparciu o kombinację powyższych atrybutów.
      4. Raporty muszą mieć możliwość grupowania zdarzeń per użytkownik, źródło zapytań (proxy, agent, sieć IP), oryginalne źródło zapytania (prywatny adres IP z sieci LAN lub nazwa komputera z oprogramowaniem SOR DNS Agent).

Ponadto SOR DNS Cloud musi zapewniać funkcję wysyłania danych źródłowych (zapytań DNS, zdarzeń bezpieczeństwa) do systemu SIEM znajdującego się w sieci Zamawiającego. Dane te muszą być przesyłane w formacie CEF i LEEF w postaci komunikatów syslog.

* 1. Dostęp do portalu klienta musi opierać się na określonych prawach dostępu, takich jak dostęp tylko do odczytu lub dostęp administracyjny. Zmiany w konfiguracji usługi DNS muszą być rejestrowane w dzienniku dostępnym dla Zamawiającego.

1. Wymagania dotyczące Usługi Wdrożenia

Wymagany zakres prac wdrożeniowych realizowanych przez Wykonawcę:

* 1. Przygotowanie i uzgodnienie z Zamawiającym projektu technicznego, w którym zostanie określona:
     1. Analiza infrastruktury DNS Zamawiającego oraz identyfikacja zagrożeń i potrzeb zabezpieczeń
     2. Architektura i konfiguracja SOR DNS w infrastrukturze SBŁ,
     3. Role i uprawnienia użytkowników,
     4. Polityki bezpieczeństwa,
     5. Planu wdrożenia opisującego proces wdrażania oferowanego rozwiązania.
  2. Uruchomienie i konfiguracja systemu SOR DNS zgodnie z najlepszymi praktykami i we współpracy z Zamawiającym:
     1. Wraz z dostawą subskrypcji SOR DNS Cloud oraz licencji na Oprogramowanie, Wykonawca zobowiązany jest do dostarczenia dokumentów potwierdzających spełnianie przez SOR DNS wymogów/parametrów pod kątem wydajności, oraz norm bezpieczeństwa przewidzianych dla rozwiązań typu SaaS (certyfikatu potwierdzającego audyt bezpieczeństwa platformy)
     2. Konfiguracja systemu SOR DNS zgodnie z projektem technicznym,
     3. Uruchomienie usługi SOR DNS Cloud w uzgodnionej konfiguracji,
     4. Uruchomienie serwerów SOR DNS Proxy we wskazanych przez Zamawiającego lokalizacjach w ilości nieprzekraczającej 20 lokalizacji,
     5. Instalację agentów SOR DNS Agent na urządzeniach wskazanych przez Zamawiającego w liczbie nie przekraczającej 25 urządzeń,
     6. Konfiguracja i uruchomienie ochrony ruchu DNS dla wskazanej grupy stacji klienckich w oparciu o konfigurację do pracy z SOR DNS Agent oraz SOR DNS Proxy,
     7. Uruchomienie funkcji analitycznych i raportowania,
     8. Monitorowanie poprawności pracy uruchomionego systemu SOR DNS,
     9. Korekty i naprawę błędów wykrytych w trakcie monitorowania oraz zgłaszanych przez użytkowników,
     10. Przegląd i podsumowanie procesu wdrożenia z Zamawiającym.
     11. W ramach akceptacji systemu SOR DNS Zamawiający przeprowadzi test wykrywania eksfiltracji danych protokołem DNS. Test zostanie przeprowadzony za pomocą niestandardowego skryptu generującego 20 serii zapytań, nie mniej niż 500 i nie więcej niż 1000 zapytań DNS w każdej serii i w odstępie około 2,5-3,5 sekundy pomiędzy seriami, w ramach których zostanie przeprowadzona eksfiltracja danych.
  3. Przygotowanie i uzgodnienie dokumentacji powdrożeniowej, tj:
     1. Wdrożona Architektura i konfiguracja systemu SOR DNS w infrastrukturze SBŁ,
     2. Wdrożone Role i uprawnienia użytkowników,
     3. Wdrożone Polityki bezpieczeństwa,
     4. instrukcji dla analityka bezpieczeństwa,
     5. instrukcji dla administratora.
  4. Wdrożenie w zakresie VII.1, VII.2 oraz VII.3 będzie realizowane przez Zespół Projektowy. Zamawiający oddeleguje osoby do współpracy z Wykonawcą w tym zakresie i w maksymalnej pracochłonności 25 Roboczodni po stronie Zamawiającego (przez „Roboczodzień” Zamawiający rozumie czas pracy jednej osoby w ciągu jednego Dnia Roboczego wynoszący osiem godzin, przy czym jeżeli praca angażuje więcej osób, to pracochłonności poszczególnych osób sumują się). Odpowiedzialność i ciężar prac leżą po stronie Wykonawcy i jest on zobowiązany do zrealizowania Wdrożenia w ramach określonej powyżej maksymalnej pracochłonności po stronie Zamawiającego, przy czym:
  5. Prace po stronie Zamawiającego, które będą wliczane do pracochłonności po stronie Zamawiającego to:
     + 1. Przeprowadzenie pełnej inwentaryzacji infrastruktury DNS na potrzeby analizy przez Wykonawcę.
       2. Dostarczenie wyników inwentaryzacji w formie raportu do Wykonawcy.
       3. Udział Zamawiającego w analizie infrastruktury DNS realizowanej przez Wykonawcę.
       4. Identyfikacja zagrożeń i potrzeb zabezpieczeń we współpracy z Wykonawcą.
       5. Udział Zamawiającego w przeglądach dokumentacji przygotowanej przez Wykonawcę.
       6. Udział w testach i odbiorach zgodnie z zapisami w Umowie.
       7. Asysta Zamawiającego przy wykonywaniu konfiguracji urządzeń lub systemów wymagających użycia uprawnień, którymi dysponuje wyłącznie Zamawiający.
       8. Pomoc Zamawiającego we wdrożeniu i konfiguracji SOR DNS realizowanych przez Wykonawcę.
  6. Prace po stronie Zamawiającego, które nie będą wliczane do pracochłonności po stronie Zamawiającego to:
  7. Prace polegające na przygotowaniu infrastruktury po stronie Zamawiającego niezbędnej do realizacji wdrożenia.
  8. Dystrybucja oprogramowania na stacje robocze z wykorzystaniem mechanizmów MS Intune.
  9. Nadzór Zamawiającego nad wdrożeniem i konfiguracją SOR DNS realizowanym przez Wykonawcę.
  10. Udział Zamawiającego w warsztatach, o których mowa w VII.5 OPZ.
  11. Współpraca w zakresie udostępniania informacji niezbędnych do wdrożenia SOR DNS.
  12. Praca osoby koordynującej działania po stronie Zamawiającego oraz monitorującej postępy prac.
  13. Wykonawca zapewnia co najmniej jednego oddelegowanego do świadczenia prac wdrożeniowych Konsultanta albo zespół konsultantów, który bierze stały udział w  pracach i ma nad nimi nadzór. Konsultant albo zespół konsultantów musi/muszą mieć wiedzę i  doświadczenie we wdrażaniu narzędzi do ochrony ruchu DNS, potwierdzoną następującymi certyfikatami:

1. potwierdzony przez producenta certyfikat inżyniera do wdrażania narzędzi do ochrony ruchu DNS oraz
2. niezależna certyfikacja cyberbezpieczeństwa (CISSP lub CEH lub OSCP).

Przy czym w przypadku zespołu konsultantów istotnym jest, aby w skład zespołu wchodziły osoby, które łącznie będą posiadać ww. certyfikaty.

* 1. W przypadku wystąpienia w trakcie świadczenia Usługi Wdrożenia jakichkolwiek trudności z winy Wykonawcy, które skutkować będą niepoprawną pracą bądź przerwami w ciągłości działania systemów lub usług SBŁ, w szczególności:

1. przerwami w działaniu systemów spowodowanych zakłóceniem działania usługi DNS,
2. przerwami w filtrowaniu i ochronie ruchu DNS,
3. przerwami w monitorowaniu i raportowaniu wykrywanych nieprawidłowości   
   i zagrożeń

na Wykonawcę zostaną nałożone kary umowne, określone w Umowie.

* 1. Przeprowadzenie warsztatów dla Zamawiającego:
     1. Na warsztatach może uczestniczyć min. 10 wskazanych przez Zamawiającego osób, będącymi pracownikami z jednostek Sieci Badawczej Łukasiewicz,
     2. Warsztaty odbędą się w formule online,
     3. Warsztaty zostaną nagrane w postaci materiału wideo do późniejszego odtworzenia przez Zamawiającego i tylko na użytek wewnętrzny,
     4. Warsztaty będą trwać min. 5 godzin zegarowych,
     5. Warsztaty odbędą się między godzinami 9:00 a 16:00, w Dni robocze,
     6. Warsztaty odbędą się na instancji SOR DNS w środowisku SBŁ na rzeczywistych danych,
     7. W ramach warsztatów zostanie przedstawiona funkcjonalność narzędzia do ochrony ruchu DNS w zakresie wdrożenia, jak w punkcie VII.2,
     8. Warsztaty zostaną przeprowadzone przez Trenera Wykonawcy, posiadającego doświadczenie w zakresie prowadzenia warsztatów z zakresu rozwiązań do ochrony usługi DNS i który w ostatnich trzech latach przez upływem terminu otwarcia ofert wykonał minimum 5 usług prowadzenia warsztatów z zakresu rozwiązań do ochrony ruchu DNS.

1. Wymagania dotyczące Usługi Utrzymania
   1. Wykonawca zapewni Usługę Utrzymania dla uruchomionego rozwiązania. Usługa będzie realizowana co najmniej w Dni robocze w godzinach 8:00-16:00, w języku polskim. Usługa Utrzymania będzie standardowo świadczona zdalnie, natomiast w przypadku braku możliwości rozwiązania problemu zgłoszenia zdalnie, będzie realizowana poprzez świadczenie jej na miejscu, w zlokalizowanych na terenie Polski jednostkach SBŁ, których zgłoszenie dotyczy, lub w których istnieje możliwość jego rozwiązania. Jednostki SBŁ zlokalizowane są na terenie Aglomeracji Łódzkiej, Aglomeracji Górnośląskiej, Aglomeracji Warszawskiej, Aglomeracji Krakowskiej, Aglomeracji Trójmiejskiej, Aglomeracji Wrocławskiej, Aglomeracji Poznańskiej oraz w Opolu, Kędzierzynie-Koźlu, Legnicy, Toruniu, Puławach i Radomiu. Ze względu na rozwój Sieci Łukasiewicz lista lokalizacji może ulec zmianie.
   2. Usługa Utrzymania obejmuje obsługę zgłoszeń następujących kategorii:
      1. błędów i usterek,
      2. weryfikacji poprawności działania systemu SOR DNS na zgłoszenie Zamawiającego,
      3. potrzeby konsultacji i wsparcie w zakresie analizy zdarzeń bezpieczeństwa,
      4. potrzeby konsultacji i wsparcie w realizacji zmian w konfiguracji w zakresie uzgodnionym z administratorami SBŁ wskazanymi przez Zamawiającego.
   3. Wykonawca zapewni poziom Usług Utrzymania w zakresie obsługi zgłoszeń zgodnie   
      z tabelą i opisem poniżej:

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria zgłoszenia** | **Maksymalny czas reakcji**\* | **Maksymalny czas naprawy\*\* lub uruchomienia rozwiązania zastępczego** | **Maksymalny czas realizacji zgłoszenia** |
| Błąd krytyczny | do 8 godzin roboczych | do 16 godzin roboczych | nie dotyczy |
| Błąd poważny | do 8 godzin roboczych | do 32 godzin roboczych | nie dotyczy |
| Usterka | do 8 godzin roboczych | do 48 godzin roboczych | nie dotyczy |
| Weryfikacja poprawności działania SOR DNS | do 8 godzin roboczych | nie dotyczy | do 32 godzin roboczych |
| Konsultacje i wsparcie w zakresie analizy zdarzeń bezpieczeństwa | do 8 godzin roboczych | nie dotyczy | do 40 godzin roboczych |
| Konsultacje i wsparcie w realizacji zmian w konfiguracji | do 8 godzin roboczych | nie dotyczy | Do 48 godzin roboczych |

**\*Czas reakcji** - czas liczony od momentu przekazania przez Zamawiającego zgłoszenia   
w ramach Usługi Utrzymania do momentu potwierdzenia mailowo przez Wykonawcę przyjęcia zgłoszenia i przystąpienia do realizacji zgłoszenia;

**\*\* Czas naprawy** – czas liczony od rejestracji przez Zamawiającego zgłoszenia w ramach Usługi Utrzymania do jego rozwiązania lub dostarczenia Rozwiązania zastępczego, umożliwiającego realizację procesów SZLKZ dotkniętych błędem; w przypadku konsultacji czas naprawy jest czasem udzielenia odpowiedzi na zadane pytanie lub udzielania wsparcia;

**Błąd krytyczny** - błąd po stronie Oprogramowania lub inna nieprawidłowość Oprogramowania lub jego konfiguracji, uniemożliwiająca użytkownikom korzystanie z usługi lub jej fragmentu, w szczególności usługi tworzenia backupów i ich odtwarzania, zarówno w całości jak i w części, a także naruszenie bezpieczeństwa usługi (dostęp do danych lub funkcji usługi z pominięciem mechanizmów zabezpieczeń);

**Błąd poważny** - nieprawidłowość działania usługi, która wpływa w istotny sposób na wyniki pracy, ogranicza funkcjonalność usługi, w wyniku czego praca jest utrudniona, ale możliwa;

**Usterka** – drobna uciążliwość, która nie wpływa w sposób istotny na działanie usługi i nie utrudnia pracy;

**Rozwiązanie zastępcze** – rozwiązanie zapewniające tymczasowe przywrócenie funkcjonalności SOR DNS utraconej wskutek wystąpienia Błędu lub Usterki, bez rozwiązywania właściwego problemu, które pozwala użytkownikom SOR DNS, pomimo istnienia nieprawidłowości, na korzystanie z SOR DNS w inny niż opisany w Dokumentacji sposób i które nie wpływa w sposób istotny na działanie SOR DNS i nie utrudnia pracy. Rozwiązanie docelowe powinno być dostarczone w czasie 48 godzin roboczych liczonych od rejestracji przez Zamawiającego zgłoszenia w ramach Usługi Utrzymania, przy czym czas ten będzie wydłużony o czas potrzebny na rozwiązanie przyczyn błędu nie leżących po stronie Wykonawcy, w szczególności: czas naprawy środowiska sprzętowo-systemowego po stronie Zamawiającego, czas oczekiwania na okno serwisowe po stronie Zamawiającego, czas naprawy błędu przez producenta Oprogramowania.

* 1. W ramach Usługi Utrzymania, Wykonawca zobowiązany jest zapewnić Zamawiającemu dostęp do dedykowanego przedstawiciela Wykonawcy pełniącego funkcję Opiekuna Technicznego Klienta (z ang. technical account manager / customer success specialist). Zadaniem Opiekuna Technicznego Klienta jest monitorowanie Usługi Utrzymania zarówno poprzez nadzór nad pracą osób świadczących bezpośrednio Usługi Utrzymania ze strony Wykonawcy, jak i poprzez regularny kontakt z Zamawiającym i proaktywne działania zmierzające do utrzymywania określonego poziomu SLA.
  2. Zamawiający ma mieć możliwość przesyłania zgłoszeń co najmniej na adres mailowy Opiekuna Technicznego Klienta ze strony Wykonawcy. Wykonawca ma przedstawić raporty z obsługi tych zgłoszeń, w szczególności SLA, na żądanie Zamawiającego.
  3. Wykonawca zobowiązany jest do świadczenia wsparcia pouruchomieniowego   
     w okresie dwóch miesięcy od wdrożenia Systemu SOR DNS w wymiarze określonym potrzebami Zamawiającego, lecz nie większym niż limit określony w pkt. VIII.7. W ramach wsparcia pouruchomieniowego Wykonawca będzie udzielał Zamawiającemu pomocy w początkowej fazie eksploatacji systemu, w szczególności:
* diagnostyki pracy SOR DNS
* administracji SOR DNS
* doszkalania pracowników Zamawiającego w uzgodnionym zakresie
* konsultacji dotyczących SOR DNS i wykraczających poza zakres jak określono   
  w VIII.3
  1. Maksymalna łączna liczba godzin do wykorzystania na świadczenie wsparcia pouruchomieniowego wynosi 200 godzin roboczych (1 h = 60 minut). Zamawiający nie jest zobowiązany do zlecania ww. czynności (uprawnienie Zamawiającego). Wykonawcy nie przysługuje żadne roszczenie za ich niezrealizowanie, w tym roszczenie o utracone korzyści.

1. Prawo opcji.

**Opcja dodatnia:** Wykonawca zobowiązany jest do zapewnienia opcjonalnej dostawy subskrypcji SOR DNS Cloud oraz licencji na Oprogramowanie dla maksymalnie 1000 użytkowników, o funkcjonalnościach zgodnych z opisem zawartym w OPZ, wraz ze Wsparciem Technicznym. Zamawiający ma prawo złożyć oświadczenie o skorzystaniu z prawa opcji w okresie 12 miesięcy od daty prawidłowej dostawy subskrypcji w ramach zamówienia podstawowego. Subskrypcje SOR DNS Cloud oraz licencje na Oprogramowanie dostarczone w ramach prawa opcji, będą obowiązywały od początku miesiąca kalendarzowego następującego po miesiącu, w którym zostało złożone oświadczenie o skorzystaniu z prawa opcji, z zastrzeżeniem że Zamawiający zobowiązany jest złożyć ww. oświadczenie nie później niż w terminie 7 Dni Roboczych przed zakończeniem miesiąca. Potwierdzeniem odbioru zamówienia w ramach prawa opcji będzie podpisany bez zastrzeżeń przez Strony Protokół odbioru.

**Opcja ujemna:** W przypadku dostawy subskrypcji posiadanego obecnie przez Zamawiającego systemu, tj. BloxOneTreat Defense Business Cloud, Zamawiający może skorzystać z prawa opcji polegającego złożeniu oświadczenia o rezygnacji z Usługi Wdrożenia opisanej w punkcie VII oraz ze świadczenia wsparcia pouruchomieniowego w zakresie opisanym w punkcie VIII.6. Zamawiający ma prawo złożyć oświadczenie o skorzystaniu z prawa opcji najwcześniej następnego dnia po zawarciu Umowy, a najpóźniej do 10 Dnia Roboczego od dnia podpisania Umowy.