**Załącznik nr 1 do Umowy nr …… z dnia ……..**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest dostarczenie i wdrożenie rozwiązania informatycznego obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS

# STOSOWANE DEFINICJE

* 1. **Dokumentacja** – Dokumentację Projektową praz Dokumentację Powykonawczą;
  2. **Dokumentacja Projektowa** – Projekt Wdrożenia Systemu, w tym Dokumentacja Testów Akceptacyjnych;
  3. **Dokumentacja Testów Akceptacyjnych** – opis działań, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z OPZ i Umową;
  4. **Dokumentacja Powykonawcza** – dokumentacja spełniająca wymogi określone w pkt II.c.2 OPZ;
  5. **Gwarancja** – gwarancja jakości obejmująca w szczególności usługi gwarancyjne, udzielona przez Wykonawcę na System, której warunki określa § 8 i § 9 Umowy oraz OPZ;
  6. **SIWZ** – Specyfikacja Istotnych Warunków Zamówienia ogłoszona w postępowaniu prowadzonym pod nazwą „Dostawa rozwiązania informatycznego obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS” znak WZP-421- […………………]
  7. **Umowa –** Umowa o udzielnie zamówienia publicznego, którego dotyczy niniejszy OPZ, zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi Załącznikami oraz Aneksami.
  8. **Jednostka** – jednostka organizacyjna sądu powszechnego, w tym Zamawiający – Sąd Apelacyjny w Krakowie, na rzecz których zawarta została Umowa, wskazana w Wykazie jednostek stanowiącym Załącznik nr [……………..] do Umowy; Zmiana Wykazu nie wymaga aneksu do Umowy, a jedynie pisemnego powiadomienia Stron
  9. **Odbiorca** – Ministerstwo Sprawiedliwości, na rzecz którego prowadzone jest postępowanie;
  10. **Oferta** - oferta złożona przez Wykonawcę w ramach postępowania o udzielenie zamówienia publicznego na świadczenia objęte niniejszą Umową, stanowiąca załącznik nr 10 do Umowy;
  11. **OPZ** – niniejszy Opis Przedmiotu Zamówienia wraz z załącznikami;
  12. **Oprogramowanie** – całość programów komputerowych, aplikacji oraz wszelkiego pozostałego software’u, w tym w szczególności oprogramowanie agentów instalowanych na stacjach końcowych lub serwerach oraz całość usług lub usług chmurowych, w tym w szczególności SaaS oraz usług zdalnego zarządzania oprogramowaniem agentów, wchodzących łącznie w skład Systemu, bądź z nim związanych, umożliwiających realizację funkcjonalności Systemu zgodnie z Umową oraz OPZ;
  13. **System** – całość oferowanego rozwiązania zawierająca wszystkie niezbędne elementy w tym: wszystkie licencje i Oprogramowanie umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ, w tym zwłaszcza oprogramowanie agentów instalowanych na stacjach końcowych lub serwerach oraz usługi zdalnego zarządzania oprogramowaniem agentów uruchomione w modelu chmurowym (SaaS), dostarczane Odbiorcy lub Jednostkom.
  14. **Sprzęt** – wszystkie niezbędne do prawidłowego działania Systemu urządzenia fizyczne (hardware), w tym kable sieciowe i inne fizyczne elementy, na których zostanie uruchomiony System w infrastrukturze Odbiorcy (w przypadku, gdy oferowane rozwiązanie będzie zawierało Sprzęt).
  15. **Producent** – osoba fizyczna lub prawna, która wytwarza Oprogramowanie i oferuje to Oprogramowanie pod własną nazwą lub znakiem towarowym.
  16. **Usługa Chmurowa (Saas)** – Model świadczenia usługi zdalnego dostępu do Oprogramowania, w którym aplikacja jest przechowywana i wykonywana w środowisku Producenta usługi i jest udostępniana Zamawiającemu, Odbiorcy lub Jednostkom przez Internet przy zachowaniu wysokiego poziomu bezpieczeństwa danych (tj. poufności, integralności i dostępności danych).
  17. **Dni Robocze** - dni pracy Jednostki, od poniedziałku do piątku, z wyłączeniem sobót i dni ustawowo wolnych od pracy.
  18. **Zgłoszenie Serwisowe** – zgłoszenie awarii Systemu przekazane poprzez zapewnione przez Wykonawcę oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia awarii, przekazane przez osobę upoważnioną ze strony Odbiorcy, zgodne z załącznikiem nr 6 do Umowy.
  19. **Projekt Wdrożenia Systemu** – dokumentacja opisująca sposób wykonania i wdrożenia Systemu zawierająca co najmniej: opis funkcjonalny Systemu, wykaz wymaganych elementów, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnej dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia;
  20. **Protokół Odbioru Projektu** – protokół odbioru stwierdzający sposób wykonania przez Wykonawcę Dokumentacji Projektowej, sporządzony według wzoru stanowiącego załącznik nr 5 do Umowy;
  21. **Protokół Uruchomienia Usługi Chmurowej** – protokół stwierdzający uruchomienie funkcjonalności ochrony użytkowników przed zagrożeniami na bazie protokołu DNS w środowisku Producenta, sporządzony według wzoru stanowiącego załącznik nr 4 do Umowy;
  22. **Protokół Odbioru Wdrożenia Systemu** – protokół stwierdzający sposób wykonania przez Wykonawcę elementów zamówienia, które nie podlegają odbiorowi na gruncie innych protokołów, sporządzony według wzoru stanowiącego załącznik nr 3 do Umowy;

# I Przedmiot zamówienia

1. Przedmiotem zamówienia jest dostarczenie i wdrożenie przez Wykonawcę na rzecz Odbiorcy oraz Jednostek rozwiązania informatycznego obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS. Wdrożenie obejmować będzie uruchomienie Systemu, oraz konfigurację zgodnie w wymaganiami Zamawiającego w zakresie niezbędnym do poprawnego działania tego Systemu.
2. W ramach przedmiotu zamówienia stanowiącego **zamówienie** Wykonawca zobowiązuje się w szczególności:
   1. dostarczyć, wdrożyć, uruchomić i skonfigurować System;
   2. wykonać Dokumentację,
   3. wykonać transfer wiedzy dla osób wskazanych przez Odbiorcę dla co najmniej 10 osób wskazanych przez Odbiorcę z zakresu funkcjonowania dostarczonego Systemu   
      i administrowania nim w wymiarze po 8 godzin (dla każdej z osób),
   4. udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów dla 80 tysięcy użytkowników. Licencjobiorcą jest Odbiorca, a podmiotami uprawnionymi do korzystania z licencji na oprogramowania są Jednostki.
   5. przenieść na Odbiorcę autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.
   6. udzielić Odbiorcy Gwarancji na dostarczony w ramach Umowy System, w tym gwarancji na oprogramowanie, na okres 36 miesięcy od podpisania Protokołu Uruchomienia Usługi Chmurowej oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu, w ramach wynagrodzenia wynikającego z Umowy.

# II Wymagania w zakresie realizującym funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS w Ministerstwie Sprawiedliwości oraz Jednostkach Sądownictwa Powszechnego

## II a. Wymagania dotyczące oferowanego rozwiązania

1. Oferowany System będzie pochodził z oficjalnego kanału dystrybucyjnego Producenta na terenie Unii Europejskiej.
2. Wszystkie oferowane urządzenia i oprogramowanie Systemu muszą stanowić jednolite środowisko tj. współpracować ze sobą bez konieczności stosowania dodatkowych elementów nie będących standardową częścią oferowanego Systemu np. pochodzić od innego Producenta.

Powyższe nie dotyczy elementu Systemu do rejestracji Zgłoszeń Serwisowych.

1. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System, który będzie skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych użytkowników. Wymaganiem Zamawiającego jest, aby możliwość zarządzania całością Systemu możliwa była z wykorzystaniem jednej konsoli zarządzającej.
2. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
3. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
4. Zamawiający wymaga, aby wszystkie elementy dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu .
5. Żaden z elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.
6. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Odbiorcy Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Odbiorcy.

## II b. Wymagania w zakresie Gwarancji na System

1. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego awarii, oprogramowanie to musi zapewnić Odbiorcy brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Odbiorcę.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe awarii Systemu w następujący sposób:
   1. **awaria krytyczna**, tj. niedostępność Systemu dla wszystkich użytkowników: czas reakcji do   
      4 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę, czas naprawy (przywrócenia funkcjonalności systemu) do 24 godzin od chwili zgłoszenia awarii przez Odbiorcę;
   2. **awaria niekrytyczna** tj.niepowodująca niedostępności Systemu: czas reakcji do 4 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę, czas naprawy (przywrócenia funkcjonalności Systemu) do 72 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę.
   3. Wszelkie awarie będą zgłaszane przez Odbiorcę za pomocą udostępnionego przez Wykonawcę oprogramowania, o którym mowa w punkie 1 powyżej.
   4. W przypadku potrzeby wydania poprawki do Systemu przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Odbiorca może zawiesić czas usunięcia awarii niekrytycznych, maksymalnie na 40 dni kalendarzowych.
   5. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
4. aktualizację i konfigurację Systemu przez Wykonawcę,
5. rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.
6. Wykonawca w ramach udzielonej gwarancji na wezwanie i w uzgodnieniu z Odbiorcą zainstaluje poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu, udostępniane przez producenta wdrożonego Systemu.
7. W ramach udzielonej gwarancji Odbiorcy przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez producenta Systemu bez ponoszenia dodatkowych kosztów finansowych przez Odbiorcę. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Odbiorcy.

## II c. Wymagania w zakresie dokumentacji

1. Wykonawca w uzgodznieniu z Zamawiającym i Odbiorcą opracuje i dostarczy następującą Dokumentację Projektową:

a) Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: opis funkcjonalny Systemu, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji i Sprzętu niezbędnego dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia,

b) Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia.

2. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:

a) procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,

b) procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,

c) instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,

d) inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione   
z przedstawicielem Odbiorcy.

3. Dokumentacja powinna być dostarczona w wersji elektronicznej w języku polskim lub angielskim.

## II d. Wymagania w zakresie transferu wiedzy

1. W ramach wdrożenia Wykonawca umożliwi Odbiorcy w siedzibie i w środowisku Odbiorcy transfer wiedzy dla co najmniej 10 osób wskazanych przez Odbiorcę polegający na możliwości uczestniczenia ww. osób przy wdrażaniu, konfiguracji i administracji Systemem.   
   W szczególności transfer wiedzy polegać będzie na:
   1. zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
   2. udzielaniu odpowiedzi na pytania zadawane przez osoby wskazane przez Odbiorcę w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego Systemu w środowisku produkcyjnym Odbiorcy, w tym omówieniu wraz z przeprowadzeniem praktycznych scenariuszy możliwości Systemu w zakresie wykrywania, przeciwdziałania   
      i usuwania złośliwego oprogramowania,
   3. Zapewnieniu transferu wiedzy w zakresie konfiguracji Systemu i administracji Systemem, który musi być prowadzony na bieżąco w trakcie wdrożenia, lecz przed zakończeniem wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.

## II e. Wymagania w zakresie wdrożenia

1. Odbiorca dostarczy niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu (platforma wirtualna).
2. W ramach wdrożenia Systemu Wykonawca dostarczy, zainstaluje i skonfiguruje Oprogramowanie, zgodnie z zaakceptowanym przez Odbiorcę Projektem Wdrożenia.
3. Miejsca realizacji przedmiotu Umowy: ul. Czerniakowska 100, 00-454 Warszawa. Na wniosek Wykonawcy Odbiorca może wyrazić zgodę w formie elektronicznej (e-mail) lub dokumentowej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Odbiorcę.
4. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Odbiorcy.
5. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu (zgodnie z postanowieniami Istotnych Postanowień Umowy) zawierający w szczególności: odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów Akceptacyjnych.
6. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia   
   i skonfigurowania Systemu będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu (zgodnie z postanowieniami Istotnych Postanowień Umowy) zawierający   
   w szczególności:
   1. odbiór Systemu ochrony użytkowników przed zagrożeniami na bazie protokołu DNS na podstawie przeprowadzonych Testów Akceptacyjnych,
   2. odbiór Dokumentacji Powykonawczej,
   3. odbiór realizacji transferu wiedzy.

## II f. Wymagania w zakresie Systemu ochrony użytkowników przed zagrożeniami na bazie protokołu DNS.

1. Wymagania ogólne
   1. Usługa chmurowa musi udostępniać funkcjonalność rekursywnego rozwiązywania zapytań DNS dla domen internetowych.
   2. Usługa chmurowa musi przyjmować zapytania DNS:
      1. kierowane bezpośrednio na jej publiczny internetowy adres IP, z możliwością ograniczenia zakresu akceptowanych adresów źródłowych zapytań,
      2. pośrednio poprzez wirtualny serwer DNS forwarding proxy zaimplementowany w sieci wew. Odbiorcy i/lub Jednostek jako maszyna Vmware,
         1. proxy musi dodawać do zapytań DNS informację o wew. prywatnym adresie IP komputera oraz o adresie MAC komputera,
         2. proxy musi przesyłać zapytania DNS do Usługi w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.
      3. poprzez Oprogramowanie agenta DNS dostarczone wraz z Usługą Chmurową i uruchomione na komputerach pracowników Odbiorcy i/lub Jednostek,
         1. agent musi wspierać systemy operacyjne MS Windows 7, 8 i 10 oraz Mac OS w wersjach od 10.10 do 10.15 oraz 11.1,
         2. agent musi dodawać do zapytań DNS informację o nazwie komputera, adresie MAC komputera, nazwę zalogowanego użytkownika i wersję systemu operacyjnego,
         3. agent musi przesyłać zapytania DNS do usługi Bezpieczny DNS w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS,
         4. agent musi wspierać możliwość hurtowej instalacji w środowisku Active Directory przy wykorzystaniu mechanizmu GPO oraz w środowisku Apple z wykorzystaniem Apple Remote Desktop.
   3. Konfiguracja Usługi Chmurowej musi być możliwa poprzez dostępny przez Internet portal WWW.
2. Polityka bezpieczeństwa
   1. Usługa Chmurowa musi mieć możliwość podejmowania działań w odniesieniu do zapytań i odpowiedzi DNS, na podstawie zdefiniowanych przez Odbiorcę i/lub Jednostki polityk bezpieczeństwa.
   2. Możliwe działania powinny obejmować: zezwolenie na zapytanie bez logowania, zezwolenie na zapytanie z jego odnotowaniem w logach, blokowanie zapytania przy pomocy odpowiedzi NXDomain (brak takiej domeny), przekierowanie (odpowiedź ze zdefiniowanym przez Zamawiającego adresem IP, odpowiedź ze zdefiniowanym przez Odbiorcę i/lub Jednostki adresem CNAME). Przekierowanie powinno być również możliwe do strony internetowej udostępnionej przez dostawcę z możliwością jej personalizacji przez Odbiorcę i/lub Jednostki.
   3. System musi podjąć działania w oparciu o nazwę domeny w zapytaniu, nazwę 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 nie może pozwolić na ominięcie blokowania domeny przez wysyłanie określonych typów zapytań, takich jak SOA, MX lub NS.
   4. System musi umożliwiać Odbiorcy i/lub Jednostkom zdefiniowanie własnej listy domen / adresów IP, na podstawie których ma podejmować reakcję, a także musi dostarczać listę domen i adresów IP w postaci list zagrożeń określonych dalej. W przypadku list własnych Odbiorcy i/lub Jednostek system musi mieć możliwość zdefiniowania poziomu zagrożenia i pewności informacji oddzielnie dla każdej listy. System musi umożliwiać tworzenie i edycję własnych list manualnie z portalu klienta, automatycznie poprzez import z pliku CSV oraz poprzez interfejs API, aby umożliwić łatwy import zewnętrznych danych o zagrożeniach. System musi umożliwiać utworzenie min. 100 list własnych, łącznie o pojemności min. 500 000 rekordów.
   5. Usługa Chmurowa musi mieć możliwość zdefiniowania listy domen wewnętrznych Odbiorcy i/lub Jednostek, czyli takich dla których DNS forwarding proxy lub oprogramowanie agenta nie będzie przesyłać zapytań DNS do Usługi Chmurowej, ale zamiast tego prześle je do określonego wewnętrznego serwera DNS Odbiorcy i/lub Jednostek.
   6. Usługa Chmurowa musi posiadać możliwość tworzenia polityk bezpieczeństwa w oparciu o sieci do której należy komputer wysyłający zapytanie.
3. Kody do pomijania blokady
   1. System musi umożliwiać obejście blokowania domen/IP przy pomocy specjalnych kodów dostarczanych wybranym użytkownikom.
   2. Usługa Chmurowa musi umożliwiać wpisanie kodu na specjalnej stronie udostępnionej w ramach Usługi Chmurowej, na którą następuje przekierowanie zgodnie z konfiguracją polityki bezpieczeństwa
   3. Kody muszą mieć możliwość przypisania kategorii zagrożeń lub kategorii treści, których obejście umożliwiają.
4. Usługa Chmurowa musi wspierać walidację DNSSEC.
5. Listy zagrożeń
   1. Usługa Chmurowa musi zapewnić dostęp do danych o zagrożeniach cyberbezpieczeństwa przez okres co najmniej 3 lat.
   2. Dane o zagrożeniach dostarczone przez dostawcę powinny obejmować:
      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 adresów IP powiązanych z sieciami botnet,
      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,
      9. lista domen zarejestrowanych w ciągu ostatnich trzech dni. Dane dotyczące nowych rejestracji muszą pochodzić z co najmniej 500 różnych domen TLD (domen najwyższego poziomu),
   3. Dane z punktu 5.2 powinny pochodzić przynajmniej od Producenta oferowanego, w tym postępowaniu rozwiązania oraz z 2 dodatkowego źródła zewnętrznego.
   4. Listy zagrożeń muszą posiadać dane o zagrożeniach celujących w Polskę. Odbiorca dokona weryfikacji tego faktu na podstawie listy CERT.PL (<https://hole.cert.pl/domains/domains.json>) – co najmniej 66% domen z listy CERT.PL z ostatniego miesiąca musi znajdować się na listach z pkt. 5.2
   5. Wszystkie powyższe listy zagrożeń muszą być możliwe do wykorzystania w konfiguracji polityki bezpieczeństwa Usługi Chmurowej.
   6. Usługa Chmurowa musi zawierać informacje o kategorii treści dla domen i musi być w stanie na nią reagować, na przykład musi zapewniać możliwość podejmowania działań w przypadku domen hostujących treści, takie jak pornografia, hazard, sieci społecznościowe, anonimizatory, reklamy itp.
   7. Ponadto dane o zagrożeniach pochodzące od Producenta muszą być dostępne za pośrednictwem interfejsu API w formatach CSV, JSON, CEF, XML, STIX do użytku w innych systemach bezpieczeństwa, takich jak SIEM, SOAR, firewall lub SWG. Dane dostępne za pośrednictwem interfejsu API muszą również obejmować:
      1. Listę domen lookalike, czyli domen, które wyglądają podobnie do najpopularniejszych domen w Internecie (np. Gooogle.com, g00gle.com itp.). Lista musi również obejmować domeny, które używają znaków specjalnych podobnych do znaków łacińskich (tak zwane homografy IDN). Zamawiający musi mieć możliwość zdefiniowania w Usłudze Chmurowej co najmniej 10 domen, dla których algorytm będzie wyszukiwał domen podobnych,
      2. Listę domen będących celem ataków Slow-Drip DDoS (inaczej: watertorture lub PSRD – pseudo random sub domains),
      3. Listę adresów FQDN i adresów IP oferujących usługi CDN (Content Delivery Networks),
      4. Listę adresów FQDN i adresów IP oferujących publiczne usługi DNS-over-HTTPS.
   8. Dane o zagrożeniach dostępne przez API muszą dostarczać kontekstowej informacji o domenie / adresie IP, w szczególności czy zagrożenie jest związane z eksfiltracją danych, czy wpływa na dostępność systemów, czy do aktywacji zagrożenia wymagana jest interakcja użytkownika, czy wymagane są wyższe uprawnienia systemowe, czy zagrożenie samoczynnie propaguje się w sieci, jakie są używane techniki MITRE ATT&CK. Odbiorca nie wymaga aby wszystkie domeny/IP w bazie danych zawierały wszystkie ww. informacje.
   9. Należy dostarczyć licencje, które gwarantują dostęp do danych o zagrożeniach, aby chronić co najmniej 80 000 użytkowników przez okres 3 lat. Dostęp do danych nie może być ograniczony ze względu na liczbę serwerów DNS lub innych systemów bezpieczeństwa korzystających z tych danych.
6. Wykrywanie zagrożeń na bazie analizy zapytań DNS
   1. Usługa Chmurowa 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 nie może działać wyłącznie w oparciu o sygnatury dla ruchu DNS znanych narzędzi tunelujących. System 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. W ramach akceptacji systemu Odbiorca i/lub Jednostki przeprowadzą test wykrywania eksfiltracji DNS. Test zostanie przeprowadzony za pomocą niestandardowego skryptu generującego nie mniej niż 200 i nie więcej niż 500 zapytań DNS w odstępie około 2,5-3,5 sekundy.
   3. Usługa Chmurowa 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.
   4. Usługa Chmurowa musi mieć funkcję wykrywania nieznanych domen DGA i słownikowych DGA (domeny generowane z całych słów losowanych z 2-3 słowników) w zapytaniach DNS.
   5. Usługa Chmurowa musi mieć funkcję wykrywania domen fastflux.
7. W ramach portalu dla klientów dostawca musi zapewnić możliwość analizy reputacji domen, adresów IP, adresów URL. Dane o domenach/IP muszą pochodzić od dostawcy i co najmniej 2 innych dostawców danych. Narzędzie analityczne powinno bezpośrednio wyświetlać informacje o domenie / adresie IP co najmniej z bazy danych o zagrożeniach opisanej w pkt. 5.2, z usługi pasywnego DNS, whois, rankingu Alexa.
   1. W ramach Usługi Chmurowej Odbiorca i/lub Jednostki muszą mieć możliwość wykonania co najmniej 64 000 zapytań dotyczących domeny / adresu IP do jednego źródła danych w ramach zapewnianego dostępu rocznie. 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).
8. Portal Usługi 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 agenta).
9. Musi istnieć możliwość wysyłania danych źródłowych z Usługi Chmurowej (zapytań DNS, zdarzeń bezpieczeństwa) do systemu SIEM znajdującego się w sieci Odbiorcy i/lub Jednostek. Dane te muszą być przesyłane w formacie CEF i LEEF w postaci komunikatów syslog.
10. 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 Odbiorcy i/lub Jednostkek.
11. Usługa musi być świadczona z 3-letnim wsparciem Producenta i musi obejmować dostęp do dedykowanego Zamawiającemu przedstawiciela Producenta pełniącego funkcję technicznego opiekuna klienta (z ang. *technical account manager* / *customer success specialist)*.

# III Funkcjonalności Systemu zgodnie z deklaracją w ofercie Wykonawcy podlegającą ocenie w ramach pozacenowych kryteriów oceny ofert:

W zależności od treści Oferty Wykonawcy podlegającej ocenie w ramach pozacenowych kryteriów oceny ofert System będzie realizował ponadto następujące funkcjonalności:

Funkcjonalność nowo obserwowanych domen (F1):

W ramach oferowanego Systemu element służący do poprawy bezpieczeństwa i ochrony przeciwko atakom Zero-day*:*

🞎 posiada możliwość rozbudowy o funkcjonalność dostępu do listy nowo zaobserwowanych domen internetowych, czyli tych, o które pytano w Internecie po raz pierwszy w ciągu ostatnich 3 dni. Dane muszą pochodzić z systemu co najmniej 400 pasywnych czujników DNS rozmieszczonych na całym świecie. Pasywny system DNS musi posiadać dane o zapytaniach DNS z min. ostatnich 10 lat.

🞎 nie posiada ww. funkcjonalności

*\* zaznaczyć właściwe*

Funkcjonalność rozbudowy Systemu (F2):

W ramach oferowanego Systemu element służący do zarządzania usługami DNS, DHCP oraz adresacją IP*:*

🞎 posiada możliwość rozbudowy Usługi Chmurowej o funkcjonalności zarządzania usługą DNS (funkcjonalność serwera autorytatywnego, forward, delegacja), usługą DHCP oraz pełne zarządzanie przestrzenią adresową, pozwalającą na uzyskananie widoczności użytkowników w ramach uruchomionych funkcjonalności bezpieczeństwa.

🞎 nie posiada ww. funkcjonalności

*\* zaznaczyć właściwe*