OPIS PRZEDMIOTU ZAMÓWIENIA

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

STOSOWANE DEFINICJE

1) **Dokumentacja** – Dokumentacja Projektowa praz Dokumentacja Powykonawcza;
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) **SWZ** – Specyfikacja Warunków Zamówienia ogłoszona w postępowaniu prowadzonym pod nazwą „Dostawa rozwiązania informatycznego obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS oraz świadczenia innych usług”
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 sądownictwa 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 w przedmiocie zamówienia objętego niniejszą Umową, stanowiąca załącznik nr […} 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 (SaaS), w tym w szczególności 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 obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS, zawierająca wszystkie niezbędne elementy w tym: wszystkie licencje i Oprogramowanie umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ.
14) **Producent** – osoba fizyczna lub prawna oferująca Oprogramowanie pod własną nazwą lub znakiem towarowym.
15) **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).
16) **Dni Robocze** - dni pracy Jednostki, od poniedziałku do piątku, z wyłączeniem sobót i dni ustawowo wolnych od pracy.
17) **Zgłoszenie Serwisowe** – zgłoszenie Awarii Systemu przekazane poprzez zapewnione przez Odbiorcę oprogramowanie, umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii, przekazane przez osobę upoważnioną ze strony Odbiorcy, zgodne z załącznikiem nr […] do Umowy. Zgłoszenie Serwisowe staje się skuteczne (zostaje dokonane) z chwilą w prowadzenia Zgłoszenia Serwisowego do oprogramowania umożliwiającego zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii..
18) **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;
19) **Protokół Odbioru Projektu** – protokół odbioru stwierdzający sposób wykonania przez Wykonawcę Dokumentacji Projektowej, sporządzony według wzoru stanowiącego załącznik nr 4 do Umowy;
20) **Protokół Odbioru Wdrożenia Systemu** – protokół stwierdzający sposób wykonania przez Wykonawcę elementów zamówienia, które nie podlegają odbiorowi na gruncie innych protokołów, w tym stwierdzający uruchomienie funkcjonalności ochrony użytkowników przed zagrożeniami na bazie protokołu DNS w środowisku Producenta, sporządzony według wzoru stanowiącego załącznik nr […] do Umowy;
21) **Zespół Odbiorowy** – wyznaczeni przez Zamawiającego, wskazani w Umowie przedstawiciele odpowiedzialni za dokonanie odpowiednich protokolarnych odbiorów.
22) **Czas Reakcji –** czas liczony od momentu Zgłoszenia Serwisowego do chwili poinformowania Zamawiającego o podjęciu działań zmierzających do ustalenia przyczyn i dokonania Naprawy.
23) **Czas Naprawy** – czas liczony od momentu przekazania Zgłoszenia Serwisowego przez Zamawiającego do chwili dokonania Naprawy; do czasy Naprawy wliczany jest Czas Reakcji;
24) **Naprawa** – trwałe usunięcie awarii poprzez usunięcie przyczyny powstania awarii skutkujące przywróceniem pełnej sprawności Systemu po wystąpieniu awarii, w tym również zakończenie innych działań naprawczych.

25) **Awaria** – niesprawność Systemu uniemożliwiająca niezakłócone korzystanie ze wszystkich funkcjonalności Systemu. Za Awarię będzie uznawane również uszkodzenie/usunięcie danych, jeżeli zostało spowodowane okolicznościami, o których mowa w zdaniu pierwszym lub w związku z Naprawą Awarii. Awarie Systemu mogą mieć charakter Awarii Krytycznej albo Awarii Niekrytycznej.

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 z 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 max. 27 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 120 tysięcy urządzeń. Licencjobiorcą jest Odbiorca, a podmiotami uprawnionymi do korzystania z Systemu 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 Odbioru Wdrożenia Systemu 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. Oferowany System musi umożliwiać przeniesienie konfiguracji z wykorzystywanego rozwiązania Infoblox BloxOne Threat Defense.

3. System musi stanowić jednolite środowisko programowe, tj. współpracować ze sobą. Niedopuszczalne jest zastosowanie dodatkowych elementów niebędących standardową częścią oferowanego Systemu np. pochodzić od innego Producenta.
   Powyższe nie dotyczy elementu Systemu do rejestracji Zgłoszeń Serwisowych.
4. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System, który będzie skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych urządzeń. Wymaganiem Zamawiającego jest, aby zarządzanie całością Systemu możliwe było z wykorzystaniem jednej konsoli zarządzającej.
5. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
6. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
7. Zamawiający wymaga, aby wszystkie elementy dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu.
8. Żaden z elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.
9. 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 celu dokonywania, rejestrowania i obsługi, w tym monitorowania statusu Zgłoszeń Serwisowych, Odbiorca zapewni i będzie utrzymywał przeznaczone do tego narzędzie przez okres realizacji zamówienia.
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:
   3.1. **Awaria Krytyczna**, wada skutkująca nieprawidłowym działaniem Systemu powodująca albo całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje tj. funkcjonalność rozwiązywania nazw DNS, funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS: Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 24 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;
   3.2. **Awaria Niekrytyczna** wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę.
   3.3. Wszelkie Awarie będą zgłaszane przez Odbiorcę za pomocą udostępnionego przez Odbiorcę oprogramowania, o którym mowa w punkcie 1 powyżej.
   3.4. 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.
   3.5. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:

a) aktualizację i konfigurację Systemu przez Wykonawcę,

b) rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.
c) Wykonawca w ramach udzielonej gwarancji na wezwanie i w terminie uzgodnionym z Odbiorcą zainstaluje poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu, udostępniane przez producenta wdrożonego Systemu.
d) 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 uzgodnieniu z Zespołem Odbiorowym 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 niezbędnych 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. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Zespół Odbiorowy na etapie odbioru Dokumentacji Projektowej.

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 Zespołu Odbiorowego.

3. Dokumentacja powinna być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.

II d. Wymagania w zakresie transferu wiedzy

1) W ramach wdrożenia Wykonawca umożliwi Odbiorcy w siedzibie i w środowisku Odbiorcy transfer wiedzy dla max. 27 osób wskazanych przez Odbiorcę polegający na możliwości uczestniczenia ww. osób przy wdrażaniu, konfiguracji i administracji Systemem. W szczególności transfer wiedzy polegać będzie na:
   a) zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
   b) 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,

c) 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.
d) potwierdzeniem prawidłowej realizacji transferu wiedzy będzie podpisany bez zastrzeżeń przez Zespół Odbiorowy Protokół Odbioru Wdrożenia Systemu.

II e. Wymagania w zakresie wdrożenia

1. Odbiorca dostarczy niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu tj. platforma wirtualizacyjna VMware, wsparcie inżynierów IT w zakresie konfiguracji systemów leżących po stronie Odbiorcy. Zakres integracji wdrażanego Systemu z systemami Odbiorcy polegać będzie w szczególności na dostarczeniu przez Wykonawcę wymaganych do prawidłowego działania Systemu informacji o koniecznych zmianach w konfiguracji systemów Odbiorcy w postaci instrukcji, opisu konfiguracji itp.
2. W ramach wdrożenia Systemu Wykonawca dostarczy, zainstaluje i skonfiguruje System, zgodnie z zaakceptowanym przez Zespół Odbiorowy Projektem Wdrożenia.
3. Miejsca realizacji przedmiotu Umowy: ul. Czerniakowska 100, 00-454 Warszawa. Na wniosek Wykonawcy Zespół Odbiorowy 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:
   a) odbiór Systemu ochrony użytkowników przed zagrożeniami na bazie protokołu DNS na podstawie przeprowadzonych Testów Akceptacyjnych,
   b) odbiór Dokumentacji Powykonawczej,
   c) odbiór realizacji transferu wiedzy.

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

1. Wymagania ogólne

1.1 Usługa chmurowa musi udostępniać funkcjonalność rekursywnego rozwiązywania zapytań DNS dla domen internetowych.

1.2 Usługa chmurowa musi być świadczona na poziomie dostępności co najmniej 99,95% czasu rocznie.

1.3 Usługa chmurowa nie może posiadać ograniczeń związanych z ilością wysyłanych zapytań na sekundę.

1.4 Usługa chmurowa musi przyjmować zapytania DNS:

1.4.1 kierowane bezpośrednio na jej publiczny internetowy adres IP, z możliwością ograniczenia zakresu akceptowanych adresów źródłowych zapytań,

1.4.2 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,

(2) proxy musi przesyłać zapytania DNS do Usługi w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.

1.4.3 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 w wersji od minimum 10 oraz Mac OS w wersjach od minimum 11

(2) agent musi dodawać do zapytań DNS informację o nazwie komputera, nazwę zalogowanego użytkownika i wersję systemu operacyjnego,

(3) agent musi przesyłać zapytania DNS do usługi Bezpieczny DNS w sposób zaszyfrowany,

(4) agent musi wspierać możliwość hurtowej instalacji w środowisku Active Directory przy wykorzystaniu mechanizmu GPO oraz w środowisku Apple z wykorzystaniem Apple Remote Desktop.

1.5 Konfiguracja Usługi Chmurowej musi być możliwa poprzez dostępny przez Internet portal WWW.

2. Polityka bezpieczeństwa

2.1 Usługa Chmurowa musi mieć możliwość podejmowania działań w odniesieniu do zapytań i odpowiedzi DNS, na podstawie zdefiniowanych przez Odbiorcę i/lub Jednostki polityk bezpieczeństwa.

2.2 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). Przekierowanie powinno być również możliwe do strony internetowej udostępnionej przez dostawcę z możliwością jej personalizacji przez Odbiorcę i/lub Jednostki.

2.3 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.

2.4 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. 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. 50 list własnych, łącznie o pojemności min. 300 000 rekordów.

2.5 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.

2.6 Usługa Chmurowa musi posiadać możliwość tworzenia polityk bezpieczeństwa w oparciu o sieci do której należy komputer wysyłający zapytanie.
2.7 Zakres przetwarzanych danych w usłudze SaaS nie może pozwalać na identyfikację osoby fizycznej wysyłającej zapytania DNS przez dostawcę usługi SaaS, producenta oprogramowania lub Wykonawcę.

3. Kody do pomijania blokady
3.1 System musi umożliwiać obejście blokowania domen/IP przy pomocy specjalnych kodów dostarczanych wybranym użytkownikom.
3.2 Usługa Chmurowa musi umożliwiać wpisanie kodu na specjalnej stronie udostępnionej w ramach Usługi Chmurowej, na którą następuje przekierowanie zgodnie z konfiguracją polityki bezpieczeństwa
3.3 Kody muszą mieć możliwość przypisania kategorii zagrożeń lub kategorii treści, których obejście umożliwiają.

4. Usługa Chmurowa musi wspierać walidację DNSSEC.

5. Listy zagrożeń
5.1 Usługa Chmurowa musi zapewnić dostęp do danych o zagrożeniach cyberbezpieczeństwa przez okres co najmniej 3 lat.
5.2 Dane o zagrożeniach dostarczone przez dostawcę powinny obejmować:
5.2.1 lista domen internetowych związanych z atakami APT,
5.2.2 lista domen i adresów IP powiązanych ze złośliwym oprogramowaniem,
5.2.3 lista domen związanych z ransomware,
5.2.4 lista domen powiązanych ze złośliwym oprogramowaniem korzystającym z algorytmów generowania domen (DGA),
5.2.5 lista domen związanych z phishingiem,
5.2.6 lista domen nowo zarejestrowanych w ciągu ostatnich 7 dni.,
5.3 Dane z punktu 5.2 powinny pochodzić przynajmniej od Producenta oferowanego, w tym postępowaniu rozwiązania.
5.4 Listy zagrożeń muszą posiadać dane o zagrożeniach celujących w Polskę na podstawie listy CERT.PL (https://hole.cert.pl/domains/domains.json) – co najmniej połowa domen z listy CERT.PL z ostatniego miesiąca musi znajdować się na listach z pkt. 5.2
5.5 Wszystkie powyższe listy zagrożeń muszą być możliwe do wykorzystania w konfiguracji polityki bezpieczeństwa Usługi Chmurowej.
5.6 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.
5.7 Ponadto dane o zagrożeniach pochodzące od Producenta muszą być dostępne za pośrednictwem interfejsu API w jednym z następujących formatów CSV, JSON, CEF, STIX do użytku w innych systemach bezpieczeństwa, takich jak SIEM, SOAR, firewall lub SWG. Dane dostępne za pośrednictwem interfejsu API muszą również obejmować co najmniej listę adresów FQDN i adresów IP oferujących publiczne usługi DNS-over-HTTPS,
5.8 Należy dostarczyć licencje, które gwarantują dostęp do danych o zagrożeniach, aby chronić 120 tysięcy urządzeń przez okres 36 miesięcy. 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

6.1 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 3 atrybuty każdego zapytania DNS, które muszą obejmować: entropię znaków w FQDN, popularność w językach naturalnych wszystkich zestawów 2- i 3-znaków z nazwy FQDN, , częstotliwość zapytań DNS.

6.2 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.

6.3 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.

6.4 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 te muszą pochodzić co najmniej od Producenta. 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 najpopularniejszych domen w Internecie.

7.1 W ramach Usługi Chmurowej Odbiorca i/lub Jednostki muszą mieć możliwość wykonania co najmniej 35 000 zapytań dotyczących analizy (pod kątem zagrożeń bezpieczeństwa) 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:

8.1 Raporty aktywności pokazujące zapytania DNS wysłane do Usługi

8.2 Raporty bezpieczeństwa pokazujące zapytania DNS, dla których Usługa Chmurowa podjęła akcje zgodnie z polityką bezpieczeństwa.

8.3 Raporty bezpieczeństwa muszą mieć możliwość filtrowania w oparciu o: źródło zapytania, adres oryginalnego źródła zapytania, domena w zapytaniu, rodzaj w zapytaniu, klasa zagrożenia (np. Malware), rodzaj zagrożenia (np. Malware C2), poziom zagrożenia, nazwa użytkownika, podjęta akcja, lista zagrożeń, polityka bezpieczeństwa.

8.4 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 klasy SIEM.

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 rozbudowy Systemu (F1):

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

☐ posiada możliwość rozbudowy Usługi Chmurowej o dodatkowe funkcjonalności polegające na zarządzaniu usługą DNS (funkcjonalność serwera autorytatywnego, forward, delegacja), usługą DHCP oraz pełnym zarządzaniu przestrzenią adresową, pozwalającą na uzyskanie widoczności komputerów w ramach uruchomionych funkcjonalności bezpieczeństwa oferowanego Systemu, przy czym funkcjonalności te muszą pochodzić od tego samego Producenta co oferowany System.

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność wykrywania domen podobnych (F2)

W ramach oferowanego Systemu element służacy do poprawy bezpieczeństwa:

☐ posiada liste domen podobnych tzw. Lookalike, czyli domen, które wyglądają podobnie do najpopularniejszych domen w Internecie (np. Google.com > g00gle.com). 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,

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność dostarczania kontekstowej informacji o zagrożeniach (F3)

☐ dane o zagrożeniach dostarczane przez oferowany System muszą posiadać kontekstową informację, dostępną poprzez API, o domenie / adresie IP, takie jak: czy zagrożenia 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 po sieci, jakie są używane techniki MITRE ATT&CK.

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność separacji / granulacji uprawnień użytkowników (F4)

☐ W ramach oferowanego Systemu możliwość zarządzania uprawnieniami w sposób pozwalający tworzyć role użytkowników uniemożliwiające wzajemną widoczność zarządzanych urządzeń (np.

użytkownik z rolą uprawniającą do zarządzania urządzeniami z jednej instancji, nie będzie widzieć / mieć dostępu do zarządzania urządzeniami z innej instancji).

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*