OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostarczenie i wdrożenie rozwiązania informatycznego obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej, wraz z narzędziami do wykrywania infekcji, powłamaniowej mitygacji i analizy zagrożeń.

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 OPZ; w tym opis działań jakie zostały wykonane aby uzyskać potwierdzenie, że wdrożony System jest zgodny z OPZ i Umową;
5. **Gwarancja** – gwarancja jakości obejmująca w szczególności usługi gwarancyjne, udzielona przez Wykonawcę na System;
6. **Umowa –** Umowa o udzielnie zamówienia publicznego, którego dotyczy niniejszy OPZ, zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi Załącznikami oraz Aneksami.
7. **Odbiorca** – Ministerstwo Sprawiedliwości, na rzecz którego prowadzone jest postępowanie;
8. **OPZ** – niniejszy Opis Przedmiotu Zamówienia wraz z załącznikami;
9. **Moduł** – Oprogramowanie i sprzęt fizyczny, serwery i usługi pochodzące od jednego Producenta, realizujący wymagane funkcjonalności i będący częścią Systemu
10. **Oprogramowanie** – wszystkie Moduły, programy komputerowe, aplikacje , obrazy maszyn wirtualnych, serwery fizyczne, oraz wszelkie pozostałe oprogramowanie, w tym oprogramowanie instalowane na serwerach oraz całość usług, umożliwiające realizację funkcjonalności Systemu zgodnie z Umową oraz OPZ;
11. **System** – całość oferowanego rozwiązania, składającego się z wymaganych Modułów obejmującego funkcjonalność ochrony poczty elektronicznej przed zagrożeniami zawierająca wszystkie niezbędne elementy w tym: wszystkie licencje, Oprogramowanie, serwery fizyczne, umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ.
12. **Producent** – osoba fizyczna lub prawna oferująca Oprogramowanie oraz serwery pod własną nazwą lub znakiem towarowym.
13. **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 przez Internet przy zachowaniu wysokiego poziomu bezpieczeństwa danych (tj. poufności, integralności i dostępności danych).
14. **Dni Robocze** - dni pracy, od poniedziałku do piątku, z wyłączeniem sobót i dni ustawowo wolnych od pracy.
15. **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. Zgłoszenie Serwisowe staje się skuteczne (zostaje dokonane) z chwilą w prowadzenia Zgłoszenia Serwisowego do oprogramowania umożliwiającego zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii.
16. **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;
17. **Protokół Odbioru Projektu** – protokół odbioru stwierdzający sposób wykonania przez Wykonawcę Dokumentacji Projektowej
18. **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 poczty elektronicznej przed zagrożeniami w środowisku Producenta
19. **Zespół Odbiorowy** – wyznaczeni przez Zamawiającego, wskazani w Umowie przedstawiciele odpowiedzialni za dokonanie odpowiednich protokolarnych odbiorów.
20. **Czas Reakcji –** czas liczony od momentu Zgłoszenia Serwisowego do chwili poinformowania Zamawiającego o podjęciu działań zmierzających do ustalenia przyczyn i dokonania Naprawy.
21. **Czas Naprawy** – czas liczony od momentu przekazania Zgłoszenia Serwisowego przez

Zamawiającego do chwili dokonania Naprawy; do czasy Naprawy wliczany jest Czas Reakcji;

1. **Naprawa** – trwałe usunięcie awarii poprzez usunięcie przyczyny powstania awarii skutkujące przywróceniem pełnej sprawności Systemu po wystąpieniu awarii, w tym również zakończenie innych działań naprawczych.
2. **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.
3. Przedmiot zamówienia
   1. Przedmiotem zamówienia jest dostarczenie i wdrożenie przez Wykonawcę na rzecz Odbiorcy rozwiązania informatycznego obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej, wraz z narzędziami do wykrywania infekcji, powłamaniowej mitygacji i analizy zagrożeń.
   2. Wdrożenie obejmować będzie uruchomienie Systemu składającego się z minimum dwóch Modułów pochodzących od różnych Producentów w celu zwiększania możliwości ochrony poczty elektronicznej, oraz konfigurację zgodnie z wymaganiami Zamawiającego w zakresie niezbędnym do poprawnego działania tego Systemu.
   3. W ramach przedmiotu zamówienia stanowiącego zamówienieWykonawca zobowiązuje się w szczególności:
      1. dostarczyć, wdrożyć, uruchomić i skonfigurować System składający się z wymaganych Modułów;
      2. wykonać Dokumentację,
      3. wykonać transfer wiedzy dla osób wskazanych przez Odbiorcę dla 5 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 2000 użytkowników. Licencjobiorcą jest Odbiorca, a podmiotami uprawnionymi do korzystania z Systemu są wszystkie podległe Jednostki i oddziały.
      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 3 lat od podpisania Protokołu Odbioru Wdrożenia Systemu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu, w ramach wynagrodzenia wynikającego z Umowy.

Wymagania w zakresie realizującym funkcjonalność wielopoziomowej ochrony poczty elektronicznej w Ministerstwie Sprawiedliwości.

# II a. Wymagania dotyczące oferowanego rozwiązania

1. Oferowany System składać się musi z minimum dwóch Modułów i będzie pochodził tylko z oficjalnych kanałów dystrybucyjnych Producentów Modułów na terenie Unii Europejskiej.
2. Każdy Moduł stanowiący element Systemu musi stanowić jednolite środowisko programowe, tj. współpracować ze sobą bez konieczności stosowania dodatkowych elementów nie będących standardową częścią oferowanego Modułu np. pochodzić od innego Producenta.

Powyższe nie dotyczy elementu Systemu do rejestracji Zgłoszeń Serwisowych.

1. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System składający się z wymaganych Modułów. Skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych użytkowników.
2. Wymaganiem Zamawiającego jest, aby każdy Moduł posiadał tylko jedną konsolę zarządzającą.
3. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
4. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
5. Zamawiający wymaga, aby wszystkie elementy i Moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu.
6. Żaden z Modułów i elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.
7. 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**, wada skutkująca nieprawidłowym działaniem dowolnego Modułu Systemu powodująca albo całkowity brak możliwości korzystania z Modułu Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 24 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;
   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. 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 terminie uzgodnionym 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 uzgodnieniu z Zespołem Odbiorowym opracuje i dostarczy następującą Dokumentację Projektową:

1. 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,
2. 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:

1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
3. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
4. 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 5 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 blokowania dostarczenia złośliwego oprogramowania,

1. 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.
2. 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 wszystkie niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu tj. wskazany w ofercie sprzęt fizyczny, serwery, platformę wirtualizacyjną Vmware w przypadku dostawy obrazów maszyn wirtualnych, platformę fizyczną oferowanych Modułów, niezbędne okablowanie oraz 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:
   1. odbiór Systemu ochrony poczty elektronicznej wraz z wchodzącymi w skład Systemu Modułami ochrony, na podstawie przeprowadzonych Testów Akceptacyjnych,
   2. odbiór Dokumentacji Powykonawczej,
   3. odbiór realizacji transferu wiedzy.

II f. Wymagania w zakresie wielopoziomowego Systemu ochrony poczty elektronicznej.

1. **Wymagania ogólne** 
   1. Oferowany Moduł musi obejmować kompleksowe rozwiązanie gwarantujące ochronę przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising) oraz złośliwym oprogramowaniem (malware). Ochrona przed złośliwym oprogramowaniem musi być realizowana w oparciu o tradycyjne bazy sygnatur jak i również poprzez uruchamianie podejrzanego kodu w izolowanych środowiskach maszyn wirtualnych (sandbox).
   2. Moduł musiskładać się z minimum z dwóch Modułów, dwóch niezależnych Producentów w celu zapewnienia wielopoziomowej ochrony poczty elektronicznej i zwiększając szansę wykrycia niebezpiecznych wiadomości email.
   3. Zadaniem pierwszego Modułu (Moduł AntySpam) musi być zaawansowana ochrona poczty elektronicznej przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising) oraz złośliwym oprogramowaniem.
   4. Zadaniem drugiego Modułu (Moduł AntyMalware) musi być zaawansowana, dodatkowa ochrona przeciw atakom malware, APT (Advanced Persistent Threats), itp., wykorzystującego tradycyjne bazy sygnatur jak i również poprzez uruchamianie podejrzanego kodu w izolowanych środowiskach maszyn wirtualnych (sandbox).
   5. Uruchamianie podejrzanego kodu, (załączników, obiektów) w izolowanych środowiskach maszyn wirtualnych musi odbywać się lokalnie, bez wysyłania analizowanych elementów poza siedzibę Odbiorcy.
   6. Moduł AntyMalware musi bezpośrednio integrować się z posiadanym przez zamawiającego modułem EDR FireEye HX.
   7. Dostawa musi obejmować kompletny System ze wskazanymi Modułami tj. licencje na oprogramowanie, sprzęt wymagany do sprawnego funkcjonowania systemu, pełny serwis producenta dla dostarczonego sprzętu i oprogramowania, dostęp do aktualizacji sygnatur i list reputacji przez okres 36 miesięcy..
   8. Moduł musi być odpowiednio wyskalowany, aby jego wydajność i sposób licencjonowania pozwoliła na ochronę poczty elektronicznej 2000 pracowników, niezależnie od ilości posiadanych skrzynek pocztowych, adresów, aliasów, czy list dystrybucyjnych.
2. **Wymagania funkcjonalne i techniczne dla Modułu AntySpam:**
   1. Moduł AntySpam musi realizować funkcje ochrony przed spamem i zagrożeniami bezpieczeństwa w ruchu SMTP.
   2. Moduł AntySpam musi umożliwiać filtrowanie poczty zarówno przychodzącej, wychodzącej jak i komunikacji wewnętrznej miedzy różnymi domenami, dlatego musi być możliwość definiowania osobnych zestawów polityk dla każdego z kierunków przesyłania wiadomości.
   3. Moduł AntySpam musi realizować następujące funkcje bezpieczeństwa poczty elektronicznej:
      1. kontrola protokołu SMTP z uwzględnieniem jego szyfrowanych wersji SSL i TLS,
      2. ochrona przed spamem,
      3. ochrona przed szkodliwą zawartością (wirusy, malware, itp.),
      4. ochrona przed niebezpiecznymi odnośnikami URL w treści wiadomości,
   4. Architektura Modułu AntySpam musi składać się z:
      1. Centralnego serwera zarządzania Modułu AntySpam, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa poczty elektronicznej i raportowania oraz
      2. Bram (ang. Gateway) służących do egzekwowania polityk bezpieczeństwa poczty elektronicznej oraz przesyłanych danych i pracujących w trybie MTA (ang. Mail Transfer Agent).
   5. Centralny serwer zarządzania i raportowania powinien być dostarczony w postaci oprogramowania, którego instalacja musi być możliwa minimum w następujących systemach operacyjnych: Microsoft Windows Server 2016 lub Microsoft Windows Server 2019.
   6. Centralny serwer zarządzania musi umożliwiać logowanie użytkowników do Modułu z wykorzystaniem kont lub grup użytkowników z usługi katalogowej, np. Microsoft Active Directory.
   7. Centralny serwer zarządzania musi umożliwiać konfigurację uprawnień dla administratorów systemu na podstawie skonfigurowanych ról. Role muszą pozwalać przynajmniej na konfigurację następujących poziomów dostępu:
      1. Brak dostępu do wybranej funkcji systemu.
      2. Dostęp tylko do odczytu.
      3. Pełny dostęp.
   8. Integracja z usługą katalogową musi dodatkowo umożliwiać konfigurację następujących ograniczeń dostępu do centralnej konsoli podczas definiowania roli:
      1. Dostępu do raportów z danych pochodzących tylko od użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.
      2. Dostęp do logów wiadomości przesyłanych tylko od i do użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.
      3. Dostęp do wybranych kolejek wiadomości należących tylko do użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.
      4. Zarządzanie politykami przypisanymi tylko do grupy użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.
   9. Jeżeli serwer zarządzania i raportowania wymaga do działania serwera baz danych, baza musi być wspierana i dostarczona w ramach wdrożenia. Akceptowalna wersja serwera baz danych to Microsoft SQL Server 2017 lub Microsoft SQL Server 2019.
   10. Brama (ang. Gateway) musi być dostarczana na dedykowanej platformie sprzętowej, tzw. appliance tego samego producenta.
   11. Oferowany Moduł wraz z licencją musi dodatkowo pozwalać na instalację dowolnej liczby bram (appliance) w formie maszyn wirtualnych, niezależnie od liczby użytkowników.
   12. Brama (sprzętowa oraz wirtualna) musi umożliwiać konfigurację adresów IP na różnych interfejsach sieciowych. Minimalna liczba adresowalnych interfejsów sieciowych nie może być mniejsza niż trzy.
   13. Moduł AntySpam musi pozwalać na adresację interfejsów sieciowych z zachowaniem segmentacji, co oznacza że systemu musi pozwalać na następującą adresację:
       1. Adres w sieci zarządzania, interfejs sieciowy odseparowany od pozostałych sieci,
       2. Adres w sieci z dostępem do Internetu np. DMZ-Zewnętrzny, interfejs sieciowy odseparowany od pozostałych sieci,
       3. Adres z sieci wewnętrznej, np. DMZ-Wewnętrzny, wykorzystywany do komunikacji z usługami wewnątrz infrastruktury, np. serwery poczty.
   14. Segmentacja sieci Modułu AntySpam musi wykorzystywać dedykowane interfejsy sieciowe. Nie jest dopuszczalna segmentacja wykorzystująca wirtualne sieci VLAN.
   15. Moduł AntySpam musi umożliwiać wdrożenie bram w konfiguracji wysoce dostępnego klastra active-active. Moduł musi pozwalać na użycie przynajmniej 8 bram w klastrze.
   16. Bramy modułu muszą działać w postaci klastra nadmiarowego. Klaster odporny na awarie musi być dostarczony w każdej lokalizacji ( dwie fizyczne lokalizacje; dwa urządzenia w każdej lokalizacji dla całego Modułu), sumarycznie minimum 4 bramy.
   17. W przypadku kiedy Odbiorca będzie wykorzystywać usługę chmurową poczty elektronicznej Moduł musi umożliwiać rozszerzenie o integrację z usługą dostarczoną przez tego samego producenta i działającą w chmurze (system hybrydowy), której zadaniem jest wstępne filtrowanie (ang. pre-filtering) wiadomości w celu wykrycia wirusów oraz spamu w wiadomościach. Rejestracja oraz konfiguracja usługi hybrydowej musi odbywać się z centralnej konsoli zarządzania.
3. **Funkcje bezpieczeństwa ochrony poczty elektronicznej Modułu AntySpam**
   1. Moduł AntySpam musi umożliwiać wykorzystanie co najmniej dwóch funkcjonalności badania reputacji nadawców dla poczty przychodzącej. Minimalne wymagania to:
      1. Serwis Real-Time Blacklist (RBL) Spamhaus Datafeed dostarczony bez żadnych ograniczeń.
      2. Mechanizm, który oznacza jako spam tych z nadawców, dla których odsetek spamu w wiadomościach przekroczył jeden ze zdefiniowanych poziomów.
   2. Moduł AntySpam musi wykorzystywać funkcję reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie szeregu weryfikacji oraz odrzucenie połączenia w przypadku:
      1. braku rekordu PTR,
      2. niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,
      3. niezgodności rekordu PTR z rekordem A.
   3. Moduł AntySpam musi umożliwiać weryfikację czy nadawca jest autoryzowany do wysyłania wiadomości z określonym polem nadawcy w oparciu o SPF (Sender Policy Framework).
   4. W ramach tego powyższego wymagania, Moduł AntySpam musi umożliwiać odrzucenie wiadomości od nadawców z określonej domeny przynajmniej w przypadku, gdy rekord SPF dla tej domeny:
      1. nie istnieje,
      2. występuje tymczasowy lub permanentny błąd, np. rekord SPF ma błędny format,
      3. nie określa, czy host nadający jest autoryzowany do wysyłania maili z tej domeny,
      4. zezwala hostowi nadającemu na wysyłanie maili z tej domeny, aczkolwiek host nie jest tam wprost wymieniony,
      5. nie zezwala hostowi nadającemu na wysyłanie maili z tej domeny.
   5. W ramach ochrony przed atakami Directory Harvest Moduł musi umożliwiać monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu. Musi istnieć możliwość zdefiniowania przedziału czasu od 1 sekundy do 1 godziny oraz ograniczenia maksymalnej ilości połączeń i wiadomości z jednego adresu IP.
   6. Dodatkowo musi istnieć możliwość tymczasowego zablokowania na zdefiniowany czas przyjmowania wiadomości z adresów IP dla których odnotowano wiadomości zawierające określoną liczbę niewłaściwych adresatów z chronionej domeny.
   7. Moduł AntySpam musi wspierać mechanizm DKIM (DomainKeys Identified Mail) zarówno w zakresie weryfikacji sygnatury (ang. DKIM Verification) w wiadomościach odbieranych jak i wyliczania oraz umieszczania sygnatury w wiadomościach wysyłanych (ang. DKIM Signing). Moduł musi obsługiwać klucze DKIM o długości przynajmniej 2048 bity.
   8. Weryfikacja sygnatury DKIM w wiadomościach odbieranych przez bramkę Modułu musi być włączana osobno dla każdego z trzech kierunków przesyłania wiadomości:
      1. Wiadomości przychodzące
      2. Wiadomości wychodzące
      3. Wiadomości wewnętrzne (dla różnych domen)
   9. Mechanizm wyliczania i umieszczania sygnatury w wiadomościach wysyłanych przez bramkę musi umożliwiać zarządzanie zarówno kluczami kryptograficznymi jak i regułami ich użycia. Moduł musi wspierać minimum następujące funkcje podpisywania wiadomości kluczem DKIM:
      1. Algorytmy podpisywania RSA-SHA-1 lub RSA-SHA-256,
      2. Możliwość podpisywania następujących nagłówków wiadomości: From, Reply-To, Subject, Date, To, Cc.
      3. Możliwość podpisywania własnych nagłówków wiadomości.
      4. Możliwość podpisywania treści wiadomości (ang. Body) bez limitu rozmiaru wiadomości albo z ustaleniem jaki rozmiar wiadomości zostanie podpisany.
   10. Moduł AntySpam musi wspierać mechanizm DMARK (Domain-based Message Authentication, Reporting and Conformance) z możliwością aktywacji dla każdego z trzech kierunków przesyłania wiadomości osobno:
       1. Wiadomości przychodzące
       2. Wiadomości wychodzące
       3. Wiadomości wewnętrzne (dla różnych domen)
   11. Moduł AntySpam musi zawierać dedykowane mechanizmy pozwalające wykrywać i zapobiegać podszywaniu się pod nadawcę (ang. spoofing). W tym celu Moduł musi weryfikować nadawcę wiadomości poprzez co najmniej:
       1. analizę elementów wiadomości takich jak nagłówki i nadawca na kopercie wiadomości,
       2. uwzględnienie wyników działania mechanizmów weryfikacji SPF, DKIM oraz SIDV (Sender ID Validation).
   12. W ramach weryfikowania nadawcy wiadomości poprzez analizę elementów wiadomości takich jak nagłówki i nadawca na kopercie Moduł musi co najmniej porównywać czy:
       1. adres nadawcy z nagłówka From: odpowiada adresowi nadawcy na kopercie wiadomości,
       2. adres nadawcy z nagłówka From: odpowiada adresowi z nagłówka Reply-To,
       3. adres nadawcy na kopercie wiadomości odpowiada adresowi z nagłówka Reply-To.
   13. Moduł AntySpam bezpieczeństwa poczty musi oferować także warstwę ochrony Anty-Malware i musi opierać się o zbiór technologii automatycznie i regularnie aktualizowanych przez Producenta. Zakres tych metod musi co najmniej obejmować:
       1. komercyjny silnik Anty-Malware, automatycznie i regularnie aktualizowany przez jego producenta,
       2. dodatkowe metody filtracji oparte o sygnatury pochodzące z innych źródeł niż wymieniony silnik Anty-Malware,
       3. metody oparte o język Yara.
   14. Moduł AntySpam bezpieczeństwa poczty musi oferować ochronę Anty-Spam opierając się o zbiór technologii automatycznie i regularnie aktualizowanych przez producenta. Zakres tych metod musi co najmniej obejmować:
       1. reguły oparte o sygnatury spamu,
       2. reguły leksykograficzne,
       3. reguły heurystyczne.
   15. Moduł AntySpam musi posiadać wbudowany mechanizm wykrywania wiadomości komercyjnych typu „Newsletter” i umożliwiać traktowanie tych wiadomości w zależności od ustalonej przez administratora Systemu polityki.
   16. Moduł AntySpam musi zapewnić analizę załączników wiadomości w celu wykrycia ich rzeczywistego typu lub rozszerzenia.
   17. Rozpoznanie typu pliku musi odbywać się w oparciu o dostarczoną przez producenta Systemu i automatycznie aktualizowaną bazę zawierającą nie mniej niż 400 typów plików.
   18. Moduł AntySpam musi zapewnić analizę odnośników zawartych w treści oraz załącznikach wiadomości w celu zweryfikowania kategorii stron internetowych do których prowadzą.
   19. Kategoryzacja stron internetowych musi odbywać się w oparciu o dostarczaną przez producenta Modułu i automatycznie aktualizowaną bazę stron internetowych przypisanych do ponad 150 kategorii i podkategorii. Moduł musi umożliwiać następujące metody dostępu do bazy kategorii:
       1. Dostęp do centrum repozytorium URL Producenta, aktualizowany bezpośrednio z Modułu
       2. Dostęp do lokalnego repozytorium wraz z własnymi kategoriami,
   20. W przypadku wystąpienia w przetwarzanej wiadomości odnośnika prowadzącego do strony z wskazanych przez administratora kategorii stron internetowych system powinien umożliwiać:
       1. Usunięcie odnośnika z treści / tematu wiadomości
       2. Modyfikację odnośnika mająca na celu jego dezaktywację
       3. Zastąpienie odnośnika predefiniowanym tekstem z możliwością wykorzystania elementów dynamicznych.
   21. Moduł AnySpam musi oferować wbudowany moduł kwarantanny.
   22. Moduł AntySpam musi umożliwiać zarządzanie kolejkami (folderami kwarantanny) do przechowywania blokowanych wiadomości w zakresie zarządzania predefiniowanymi oraz tworzenia nowych. Wiadomości kierowane do określonych kolejek muszą być przechowywane w ramach bramy lub poza nią na zasobie dostępnym przez NFS lub Samba.
   23. Moduł AntySpam musi udostępniać mechanizm pozwalający na przeglądanie przez chronionych użytkowników kierowanych do nich wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości z kwarantanny.
   24. Dodatkowo, decyzją administratora użytkownicy muszą mieć możliwość zarządzać swoimi własnymi listami zabronionych i dopuszczonych nadawców.
4. **Definiowanie polityk Modułu AntySpam bezpieczeństwa poczty**
   1. Funkcjonalność zarządzania politykami Modułu AntySpam musi umożliwiać jednokrotne definiowanie elementów takich jak filtry i akcje a następne ich wielokrotne wykorzystywanie w politykach regułach.
   2. Możliwe do podjęcia w ramach polityk akcje muszą obejmować co najmniej:
      1. dostarczenie wiadomości z wykonaniem dodatkowych akcji:
         1. zmodyfikowanie tematu wiadomości,
         2. usunięcie i/lub dodanie nagłówka X-header,
         3. wysłanie kopii wiadomości pod wskazany adres lub adresy email,
      2. zablokowanie wiadomości (kwarantanna),
      3. zapisanie wiadomości do wskazanej kolejki,
      4. wysłanie powiadomienia, gdzie:
         1. jego nadawcą może być oryginalny nadawca, administrator lub wskazany adres
         2. jego odbiorcą może być oryginalny nadawca, oryginalny adresat, administrator, wskazany adresat lub adresaci (wszyscy z wymienionych lub dowolnie wybrani)
         3. temat i zawartość powiadomienia mogą być w pełni dostosowane do potrzeb,
         4. do powiadomienia może być dołączona oryginalna wiadomość przed lub po filtrowaniu.
   3. Każda z polityk musi składać się z reguł, które muszą być przetwarzane w kolejności „z góry na dół”, do końca listy reguł, lub do reguły, która wprowadzi akcję końcową np. zablokuj wiadomość, lub umieść w kwarantannie.
   4. Moduł AntySpam musi zawierać predefiniowane reguły co najmniej następującego typu:
      1. Ochrona antywirus / antymalware
      2. Wykrywanie typów załączników
      3. Antyspoofing
      4. Analiza odnośników
      5. Anyspam
      6. Rozpoznawanie wiadomości komercyjnych
      7. Umieszczanie informacji / zastrzeżeń w stopce lub nagłówku wiadomości
5. **Zarządzanie i raportowanie Modułu AntySpam**
   1. Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie muszą być dostępne przez zintegrowaną webową konsolę administracyjną z możliwością delegowania uprawnień do administrowania poszczególnymi składnikami i opcjami systemu.
   2. Moduł AntySpam musi posiadać funkcjonalność zarządzania bramami, zarówno serwerami sprzętowymi jak i maszynami wirtualnymi, uruchomiony na centralnym serwerze zarządzania.
   3. Centralny serwerem zarządzania, musi być obsługiwany przez przeglądarkę internetową oraz musi posiadać minimum następujące funkcje:
      1. Dostęp do stanu usług oraz stanu obciążenia wybranej bramy.
      2. Konfigurację adresów IP dla poszczególnych interfejsów bramy.
      3. Konfigurację adresów DNS wykorzystywanych przez poszczególne moduły bramy.
      4. Konfigurację tras routingu.
      5. Konfigurację kopii zapasowych.
      6. Konfigurację powiadomień SNMP.
      7. Pobieranie i instalowanie poprawek oraz nowych wersji Modułu dla skonfigurowanych grup urządzeń w sposób automatyczny. Nie jest dopuszczalne wykonywanie aktualizacji jedynie w sposób ręczny, pobierając i instalując pojedyncze poprawki.
   4. Dostęp do webowej konsoli centralnego zarządzania musi odbywać się w bezpiecznym połączeniu https.
   5. Dostęp do konsoli centralnego zarządzania bramą musi być możliwy za pośrednictwem protokołu SSH i/lub w bezpiecznym połączeniu https.
   6. Konsola musi wspierać silne uwierzytelnianie łączących się do niej administratorów z wykorzystaniem cyfrowych certyfikatów X.509.
   7. Konsola zarządzania musi zawierać ekran przedstawiający wykres sumarycznej aktywności oraz podstawowe statystki. Musi istnieć możliwość dostosowania tego widoku do własnych potrzeb. Ekran ten musi również zawierać ostrzeżenia dotyczące poprawności pracy poszczególnych komponentów oprogramowania.
   8. Centralne zarządzanie Modułu AntySpam musi być wyposażone w funkcjonalność raportującą umożliwiającą:
      1. Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem.
      2. Harmonogram musi umożliwiać generowanie raportów codziennie, co tydzień lub co miesiąc. W przypadku opcji co tydzień musi być możliwe dowolne wskazanie wybranych dni tygodnia. W przypadku opcji co miesiąc musi być możliwe dowolne wskazanie wybranych dni miesiąca np. 2, 15, 17-31.
      3. Harmonogram musi umożliwiać generowanie raportów, dla wszystkich dat, zdefiniowanego okresu lub relatywnie, czyli za okres np. ostatniego dnia, tygodnia, miesiąca w zakresie od 1 do 5 dla każdego z nich.
      4. Musi być możliwe dostarczanie raportów w postaci plików pdf, xls oraz html.
      5. Musi być możliwe dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.
   9. Centralne zarządzanie musi umożliwiać delegowanie uprawnień do zarządzania i raportowania zarówno dla użytkowników domenowych jak i użytkowników tworzonych lokalnie w Systemie.
   10. Główny administrator Moduł AntySpam musi mieć możliwość wglądu w szczegółowy audyt aktywności pozostałych administratorów zawierający następujące informacje:
       1. Data akcji,
       2. Nazwa administratora, który przeprowadził akcję
       3. Element, na którym podejmowana jest akcja,
       4. Akcja (np. zalogowanie, wylogowanie, oraz dodanie, zmiana i usunięcie obiektu),
       5. W przypadku zmiany obiektu jego poprzednia i obecna wartość.
6. **Integracje Modułu AntySpam**
   1. Moduł musi umożliwiać integrację z usługami katalogowymi. W tym zakresie wspierane muszą być co najmniej:
      1. Microsoft Active Directory
      2. LDAP Server
      3. Import listy użytkowników z odpowiednio sformatowanego pliku
   2. Moduł musi zapewnić wykorzystanie integracji z usługami katalogowymi w co najmniej następujących celach:
      1. Weryfikacja adresów pocztowych odbiorców poczty przychodzącej
      2. Uwierzytelnienie nadawcy poczty wychodzącej
      3. Uwierzytelnienie użytkownika przy dostępnie do portalu kwarantanny
      4. Weryfikacja list dystrybucyjnych
      5. Kierowanie wiadomości przychodzących (ang. mail routing) w oparciu o przynależność adresata do grup użytkowników w usłudze katalogowej.
   3. Moduł musi mieć możliwość integracji z rozwiązaniami klasy SIEM.
   4. W zakresie integracji z systemami SIEM Moduł AntySpam musi:
      1. wspierać przynajmniej następujące formaty:
         1. CEF – Common Event Format,
         2. LEEF - Log Event Extended Format,
         3. Para klucz – wartość,
         4. Własny, w oparciu o wbudowane szablony,
      2. wspierać zarówno protokół TCP oraz UDP.
      3. umożliwiać dostosowywanie i formatowanie logów osobno dla poszczególnych faz przetwarzania wiadomości, minimum:
         1. Informacje o połączeniu SMTP
         2. Informacje o wiadomości i jej przetwarzaniu przez polityki
         3. Informacje o dostarczeniu wiadomości do kolejnego serwera
         4. Akcje administracyjne (audit log)
   5. Moduł AntySpam musi umożliwiać integrację z rozwiązaniami do szyfrowania wiadomości (tzw. Email Encryption Gateway) firm trzecich.
   6. Producent Modułu AntySpam oprócz rozwiązań bezpieczeństwa poczty elektronicznej musi mieć również możliwość rozbudowy o funkcjonalność bezpieczeństwa web oraz ochrony przed wyciekiem poufnych informacji (DLP). Dzięki temu jest on w stanie w swoich laboratoriach m.in. analizować na jakie strony prowadzą odnośniki umieszone w wiadomościach email (spam), dokonywać ich kategoryzacji oraz badać na ile ich odwiedzanie jest niebezpieczne.
   7. Moduł musi umożliwiać integrację z rozwiązaniem bezpieczeństwa web tego samego producenta i być przystosowany do takiej rozbudowy.
7. **Wymagania funkcjonalne i techniczne dla Modułu AntyMalware**
   1. Analiza dynamiczna w maszynach wirtualnych i wykrywanie w załącznikach ataków nie może opierać się na analizie w rozwiązaniach typu chmurowego (poza infrastrukturą Odbiorcy), lecz na urządzeniu zainstalowanych w infrastrukturze Odbiorcy. Analiza ataku musi odbywać się za pomocą dynamicznej analizy zachowania kodu umożliwiających równoczesną analizę zagrożenia w różnych wersjach systemu operacyjnego i aplikacjach.
   2. Architektura Modułu AntyMalware musi składać się z:
      1. Centralnego serwera zarządzania Modułu AntyMalware, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa dodatkowej ochrony poczty elektronicznej i raportowania oraz
      2. Analizatorów dynamicznych służących do wykonywania głębokiej analizy w piaskownicy (sandbox) w środowisku maszyn wirtualnych oraz wykrywania zawansowanych zagrożeń poczty elektronicznej oraz pracujących w trybie MTA (ang. Mail Transfer Agent).
   3. Każdy Analizator dynamiczny musi być dostarczony w postaci urządzenia fizycznego Producenta. Urządzenie MUSI działać w oparciu o dedykowane platformy sprzętowe (appliance) dostarczane przez Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
   4. Analizatory dynamiczne Modułu AntyMalware muszą działać w postaci klastra nadmiarowego. Klaster odporny na awarie musi być dostarczony w każdej lokalizacji (( dwie fizyczne lokalizacje; dwa urządzenia w każdej lokalizacji dla całego Modułu ), sumarycznie minimum 4 analizatory.
   5. Moduł AntyMalware musi integrować się z system SIEM i zasilać go wszelkimi wykrytymi zdarzeniami bezpieczeństwa
   6. Moduł AntyMalware musi być dostarczony w postaci fizycznych urządzeń wraz z oprogramowaniem i wszystkimi niezbędnymi licencjami (z uwzględnieniem licencji niezbędnych dla maszyn wirtualnych w SandBox, w tym MS Windows, MacOS, MS Office)
   7. Każdy z Analizatorów dynamicznych musi mieć wydajność analizy minimum 8 tys. przychodzących wiadomości email na godzinę, w tym minimalnie 600 unikalnych załączników do email na godzinę.
   8. Równoległa analiza dynamiczna musi być wykonywana na maszynach wirtualnych w różnych wersjach systemu operacyjnego (minimum Microsoft Windows 7 (w wersjach zarówno 32 jak i 64 bit), Microsoft Windows 10 64-bit, Mac OS, CentOS) i aplikacji.
   9. Każdy z Analizatorów dynamicznych musi być wyposażony w co najmniej 2 interfejsy monitorujące ruch poczty email oraz dedykowany port zarządzający do podłączenia do osobnego segmentu sieci.
   10. Analizator dynamiczny musi umożliwiać wdrożenie w następujących trybach:
       1. in-line - urządzenie działa jako MTA będąc pośrednikiem w ruchu email do serwerów poczty,
       2. monitorowania - przez podłączenie do portu SPAN przełącznika sieciowego lub do urządzenia typu TAP,
       3. BCC – do urządzenia dociera kopia oryginalnych maili poprzez protokół SMTP (generowanych przez bramkę pocztową lub serwer pocztowy).
   11. Analizator dynamiczny musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa redundantne dyski pracujące w RAID.
   12. Analizator dynamiczny musi zapewnić wykrywanie zaawansowanych ataków przenoszonych w załącznikach poczty elektronicznej oraz kontrolę adresów URL umieszczanych w treści wiadomości oraz analizę samej wiadomości, przy czym:
       1. po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie złośliwego email w kwarantannie,
       2. po wykryciu nieznanego wcześniej adresu URL prowadzącego do pliku musi być możliwe automatyczne nawiązanie połączenia przez urządzenie do Internetu, pobranie pliku i przeanalizowanie go, a następnie w razie wykrycia zagrożenia, wygenerowanie alertu i zatrzymanie wiadomości email w kwarantannie,
       3. po wykryciu nieznanego wcześniej adresu URL nie prowadzącego do obiektu musi być możliwe automatyczne przekazanie go do centralnego systemu zarządzania celem korelacji z alertami generowanymi przez inne Analizatory dynamiczne.
   13. W przypadku nieznanych wcześniej adresów URL Moduł musi umożliwiać administratorowi zdefiniowanie czasu wstrzymania dostarczenia wiadomości, tak aby możliwe było ukończenie zaawansowanej, przedłużonej analizy URL po stronie dostawcy rozwiązania.
   14. Cała analiza załączników w celu wykrycia ataków w poczcie email musi odbywać się w infrastrukturze Odbiorcy.
   15. Moduł AntyMalware na potrzeby analizy dynamicznej musi wykorzystywać dedykowane środowisko wirtualne (hypervisor), a nie standardowe dostępne na rynku rozwiązania jak VMware, MS Hyper-V czy też Virtual Box.
   16. Moduł AntyMalware musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty email niezależnie od użytego rozszerzenia pliku.
   17. Moduł AntyMalware musi analizować i blokować niebezpieczne treści dla załączników takich jak:
       1. plików wykonywalnych (EXE,MSI),
       2. dokumentów (PDF, RTF),
       3. plików Java (JAR, JS, JSE),
       4. plików z pakietu MS Office,
       5. plików multimedialnych (FLASH),
       6. plików skompresowanych (RAR, ZIP, 7ZIP, GZIP, SFX),
       7. skrótów MS Windows (LNK),
       8. plików www (HTML, HTM),
       9. plików z bibliotekami (DLL),
       10. plików zawierających skrypty (Powershell, VBS, BAT, CMD, VBE, VB, COM),
   18. Moduł AntyMalware musi zostać wdrożony w trybie "in-line" w trybie aktywnego blokowania zainfekowanych wiadomości email i umieszczać je w lokalnej kwarantannie
   19. Moduł AntyMalware musi dodawać oznaczenia (X header) do nagłówków wiadomości email zależnie od akcji podjętej przez Moduł analizy (m.in. email przeskanowany bez wykrytego zagrożenia, email zawiera kod złośliwy) do wykorzystania przez inne systemy ochrony Odbiorcy i analizy wstecznej.
   20. Moduł AntyMalware musi automatycznie tworzyć reguły umożliwiające blokowanie zagrożeń na podstawie:
       1. wyników analizy malware wykonanej na danym urządzeniu,
       2. danych przekazanych z centralnego systemu zarządzania, pochodzących z wyników analizy wykonanych na innych urządzeniach Modułu AntyMalware w środowisku Odbiorcy,
       3. danych dostępnych z centralnego repozytorium producenta (centrum reputacyjne Producenta).
   21. Moduł AntyMalware musi umożliwiać stosowanie własnych reguł opisujących parametry z nagłówków wiadomości email (header) i na tej podstawie wykrywać groźne wiadomości pocztowe.
   22. Moduł AntyMalware musi posiadać dodatkowe, uzupełniające mechanizmy chroniące pocztę email Odbiorcy przed atakami:
       1. phishing / spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających),
       2. impersonation (CEO fraud) - kompromitacja kadry zarządzającej w celu kradzieży informacji,
       3. infekcją kodu JavaScript, VBScript,
       4. spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.
       5. z opóźnionym startem – w których obiekty niebezpieczne (załączniki/URL) zostają aktywowane już po dostarczeniu wiadomości – w tym wypadku Moduł musi generować alerty o niebezpiecznych wiadomościach email ,które zostały dostarczone do odbiorców (atak retroaktywny);
   23. Moduł AntyMalware musi umożliwiać deszyfrację załączników przesyłanych przez pocztę email Odbiorcy przy użyciu listy najczęściej używanych haseł lub inteligentnego wyszukiwania haseł w treści maila, w tym z opcją OCR hasła przesłanego w obrazku. Lista haseł MUSI mieć możliwość dodania haseł specyficznych dla języka polskiego z polskimi znakami.
   24. Moduł AntyMalware musi posiadać możliwość konfiguracji środowisk wirtualnych analizy dynamicznej co najmniej w zakresie: nazwy domeny, nazwy użytkownika, folderów użytkowników, ostatnio otwartych plików, historii przeglądania stron www w przeglądarce internetowej. kont FTP, Outlook i Skype w celu utrudnienia wykrycia przez analizowany malware.
   25. Moduł AntyMalware musi umożliwiać analizę wiadomości email w trybie "LIVE", to jest z możliwością połączenia malware detonowanego w środowisku wirtualnym z zewnętrznym łączem internetowym. Łącze to musi stanowić separowany link do Internetu („brudny Internet”) konfigurowany na dedykowanym porcie fizycznym Urządzenia.
   26. W wyniku analizy Moduł musi zapewniać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy wiadomości email. Wśród danych muszą się znaleźć co najmniej:
       1. adres nadawcy i adres odbiorcy,
       2. analiza nagłówka wiadomości (header)
       3. body wiadomości,
       4. wyniki analizy załączników i adresów URL,
       5. informacje kontekstowe na temat wykrywanego zagrożenia malware, adware, spyware,
       6. funkcja skrótu (HASH), przynajmniej MD5 i SHA256
   27. Moduł AntyMalware musi zapewniać dostęp do sekwencyjnego (krok po kroku) zapisu zmian wykonywanych przez analizowany niebezpieczny załącznik z wiadomości pocztowej: w rejestrze, procesach, systemie plików, sposobie startu systemu, próby nawiązania połączenia sieciowego (wraz z zapisem tych prób w postaci plików PCAP dostępnych w GUI urządzenia).
   28. Moduł AntyMalware musi posiadać graficzne przedstawienie zmian wykonywanych przez obiekt z wiadomości pocztowej (przekazany bezpośrednio lub poprzez adres URL) po analizie w środowisku wirtualnym w postaci grafu powiązań wykonywanych czynności.
   29. Moduł AntyMalware musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnej wiadomości email).
   30. Moduł AntyMalware musi posiadać dodatkowy mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
       1. skrypty przesyłane w wiadomości email,
       2. pliki wykonywalne przesyłane w załączniku lub URL,
       3. dokumenty MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym,
       4. nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO,
       5. wiadomości email ze skróconymi linkami (tiny URL),
       6. dokumenty MS OFFICE z flash,
       7. pliki JAR,
       8. hasła z formularzy przesyłanych w formie HTTP request,
       9. zaszyfrowane pliki PDF,
       10. pliki typu wygaszacz ekranu,
       11. nieznanych plików konfiguracyjnych .SettingContent-ms.
       12. zaszyfrowane dokumenty MS Office
       13. Dokumenty MS Office z obiektami Embedded Object
       14. Dokumenty PDF, HWP lub MS Office z aktywnością sieciową
       15. pliki MS Office z makrem tworzącym plik wykonywalny
       16. uszkodzone pliki wykonywalne PE
       17. obiekty próbujące wykryć rozwiązania AV/Firewall za pomocą WMI
       18. pliki z niezgodnym rozszerzeniem (innym niż w magic byte)
       19. dokumenty Office z zagnieżdżonymi obiektami SWF
   31. Moduł AntyMalware musi mieć możliwość przepisania adresów URL w przesyłanej wiadomości tak aby pomimo kliknięcia użytkownik nie był przekierowany do potencjalnie złośliwej treści. W wypadku kiedy adres URL będzie złośliwy, przedstawiony ekran informujący o blokadzie musi umożliwiać dostosowanie prezentowanych użytkownikowi komunikatów do wymagań Odbiorcy (grafika i tekst z informacją o blokadzie w języku Polskim).
   32. Moduł AntyMalware musi umożliwiać konfigurację reguł blokujących i dopuszczających bazując na wyrażeniach regularnych, w celu modyfikacji ochrony w zakresie: adresu e-mail nadawcy, domeny nadawcy, adresu IP nadawcy i adresu e-mail odbiorcy (zarówno „whitelista” jak i „blacklista”).
   33. Moduł AntyMalware musi mieć zaimplementowany mechanizm wyszukiwania analizowanych wiadomości pocztowych i filtry wyszukujące co najmniej na: adres email odbiorcy, adres email nadawcy, temat wiadomości, URL, załącznik.
   34. Moduł AntyMalware musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości email i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
   35. Moduł AntyMalware musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie Yara.
   36. Moduł AntyMalware musi umożliwiać generowanie raportów zawierających co najmniej:
       1. statystyki wykrytych alertów, typy i opis wykrytych zagrożeń, akcje podjęte w związku z wykrytym zagrożeniem,
       2. statystyki przeanalizowanych wiadomości email,
       3. statystyki analizowanej poczty, z podziałem na poszczególne godziny, w celu oceny obciążenia systemu
   37. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
   38. Moduł AntyMalware musi generować automatycznie (za pomocą wbudowanej funkcji) raport z analizy dynamicznej do pliku PDF, zarówno dla graficznej reprezentacji wyniku analizy jaki i wykonanych po sobie czynności krok po kroku.
   39. Moduł AntyMalware musi umożliwiać przesyłanie do zewnętrznego odbiorcy (typu SIEM/Log Collector) metadanych o wszystkich procesowanych wiadomościach e-mail (szkodliwe i nieszkodliwe); eksport musi być możliwy za pomocą minimum rsyslog oraz formatu json (http listener).
   40. Metadane muszą uwzględniać takie informacje, jak: rozmiar wiadomości, werdykt analizy, domenę nadawcy, nagłówki wiadomości (header), pola to/cc/bcc, temat, messageid; jeśli wiadomość zawiera załącznik, to dodatkowo metadane muszą opisywać takie parametry jak: rozmiar załącznika, sumy kontrole MD5 oraz SHA256, nazwę załącznika oraz werdykt analizy
   41. Moduł AntyMalware musi zapewniać system powiadamiania o przeciążeniach wynikających ze zbyt dużej ilości wiadomości email do analizy. Gdy liczba wiadomości e-mail w kolejce oczekiwania na analizę osiągnie 30% progu przeciążenia, Moduł musi generować powiadomienie o statusie ostrzegawczym. Gdy liczba wiadomości e-mail w kolejce osiągnie 70% progu przeciążenia, Moduł musi generować powiadomienie o statusie krytycznym.
   42. Alarmy generowane przez system na bazie analizy dynamicznej w maszynach wirtualnych muszą obejmować mapowanie MITRE, wskazujące na technikę/techniki MITRE zidentyfikowane w ramach analizy danej próbki.
8. **Wymagania funkcjonalne i techniczne dla analizatora zasobów plikowych Modułu AntyMalware**
   1. W ramach dostawy modułu AntuMalware musi być także dostarczony analizator zasobów plikowych, pozwalający na masową detonacje i weryfikacje plików, obiektów przechowywanych na serwerach plikowych i macierzach. Analizator plikowy ma za zadanie wykonywać analizę dynamiczną w środowisku maszyn wirtualnych plików pochodzących m.in. z komunikacji email (załączniki) które nie zostały wykryte na etapie przesyłania wiadomości, a mogą przenosić złośliwy kod, malware itp.
   2. Analizator plikowy musi mieć możliwość analizy repozytoriów plikowych w celu znalezienia złośliwego oprogramowania (typu malware, exploit, itp).
   3. Wykrywanie ataków musi odbywać się przez dedykowane fizyczne urządzenie przeznaczone do instalacji w szafie RACK.
   4. Analizator plikowy musi być wyposażone w co najmniej 4 interfejsy miedziane 1Gb/s.
   5. Analizator musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa dyski redundantne pracujące w RAID.
   6. Analizator musi mieć wydajność umożliwiającą skanowanie co najmniej 60 000 analiz unikalnych obiektów dziennie wykazanych w specyfikacji Producenta.
   7. Analizator plikowy musi wykonywać analizę dynamiczną (sandbox) w równoległym środowisku (uruchamianym jednocześnie) maszyn wirtualnych.
   8. Analizator musi działać w oparciu o dedykowane platformy sprzętowe (urządzenia fizyczne) dostarczane przez Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
   9. Analizator musi wykonywać skanowanie udziałów plikowych: ciągłe, zaplanowane i na żądanie oraz poddawać kwarantannie złośliwe oprogramowanie odnalezione na zasobach plikowych
   10. Analizator plikowy musi umożliwiać tworzenie niezależnych skanowań (zadań skanowania) dla podłączonych repozytoriów plikowych (zasobów plikowych).
   11. Analizator musi mieć możliwość skanowania i filtrowania tylko wskazanych typów plików do skanowania.
   12. Analizator musi umożliwiać zatrzymanie i wznawianie skanowania.
   13. Analizator musi mieć możliwość przenoszenia niezłośliwych plików do wskazanego zasobu, a złośliwych plików do oddzielnego zasobu kwarantanny.
   14. Analizator musi być w stanie przywrócić plik do jego pierwotnej lokalizacji po zwolnieniu go z kwarantanny.
   15. Analizator musi być w stanie dostarczać raporty analityczne z informacjami o zachowaniu pliku - zaangażowanych procesach, dostępie do plików / zapisie na dysku, zmianach w rejestrze.
   16. Analizator musi oferować możliwość filtrowania zadania skanowania na podstawie typu pliku oraz daty modyfikacji.
   17. Analizator musi posiadać oprócz silnika analizy dynamicznej, silnik analizy statycznej.
   18. Analizator musi mieć możliwość analizy plików do 1024 MB. Maksymalny rozmiar plików, które będą skanowane, musi być konfigurowalny.
   19. Analizator musi mieć możliwość analizowania plików .eml (wiadomości email zapisane do pliku)
   20. Analizator musi obsługiwać natywną integrację z Microsoft SharePoint w trybie online, aby zapewnić bezpieczne udostępnianie plików.
   21. Analizator musi wspierać skanowanie i ochronę dla następujących typów repozytoriów plikowych: CIFS, NFS, WebDAV, Secure WebDAV.
   22. Analizator musi mieć możliwość analizy malware w formatach co najmniej:, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
   23. Funkcjonalność analizy obiektów musi realizować statyczną analizę (analizę cech) i dynamiczną analizę (analizę zachowania po uruchomieniu środowisku wirtualnym) podejrzanych obiektów zebranych z analizowanego ruchu.
   24. Analizator musi na potrzeby analizy dynamicznej wykorzystywać środowisko wirtualne (hypervisor), przy czym:
       1. środowisko, w jakim jest wykonywana analiza dynamiczna, musi posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware,
       2. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku muszą posiadać mechanizmy symulacji realnego użytkownika (w tym co najmniej: ruchy myszą, historię odwiedzanych stron web, pliki cookies).
   25. Analizator musi posiadać możliwość konfiguracji środowisk wirtualnych co najmniej w zakresie: nazwy domeny, nazwy użytkownika, folderów użytkowników, ostatnio otwartych plików, historii przeglądania stron www w przeglądarce internetowej oraz kont FTP, Outlook i Skype w celu utrudnienia wykrycia przez analizowany malware.
   26. Analiza zachowania i cech ataku musi się odbywać z poziomu hypervisora – nie może być wymagane instalowanie dodatkowych procesów/agentów monitorujących wewnątrz maszyn wirtualnych.
   27. Maszyny wirtualne z różnymi systemami operacyjnymi i aplikacjami muszą być dostarczone wraz z urządzeniami i okresowo aktualizowane przez producenta i nie mogą wymagać dodatkowych licencji wymaganych do konfiguracji po stronie Odbiorcy.
   28. Sposób działania maszyn wirtualnych musi umożliwiać wykonanie analizy zachowania obiektów PDF, Java, MS Office z użyciem kilku wersji tych aplikacji bez uruchamiania dodatkowych maszyn wirtualnych.
   29. Analiza ataku musi umożliwiać wykrywanie zagrożeń typu kernel rootkit, code injection, DLL injection.
   30. W wyniku analizy Analizator musi zapewniać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy. Wśród tych danych muszą się znaleźć co najmniej: adresy URL jeśli są związane z analizowanym malware, funkcje skrótu (hash) MD5 oraz wykryty plik malware.
   31. Analizator musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnym ruchu).
   32. Analizator musi umożliwiać wykrywanie wszystkich faz zaawansowanych ataków: exploit, dropper/malware, callback oraz lateral movement.
   33. Analizator wykonując analizę zagrożeń musi umożliwiać generyczne (bez wcześniejszej znajomości złośliwego kodu) wykrywanie ataków typu exploit, w tym nowych exploit, nie znanych wcześniej.
   34. Wykrywanie exploit musi się odbywać po analizie co najmniej takich formatów plików jak Java Script, zakodowany (obfuscated) Java Script, obiekty Flash, PDF, pliki graficzne, pliki multimedialne mp3/mp4, pliki MS Office, Java.
   35. Informacja o wykryciu fazy exploita musi być wskazana w zapisie sekwencyjnym z analizy dynamicznej ataku.
   36. Analizator musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
   37. Analizator musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Odbiorcę, opisujących cechy podejrzanych obiektów w formacie YARA.
   38. Analizator musi posiadać dodatkowy mechamizn wykrywania zdarzeń typu "prawdopodobny malware" (takich jak zaszyfrowane dokumenty MS Office, zdegradowane pliki wykonywalne Windows PE, formularze web przekazujące hasła, pliki niewykonywalne umożliwiające komunikację do niestandardowego portu). Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
   39. Analizator musi generować wynik analizy dynamicznej przynjamniej do pliku PDF.
   40. Analizator musi umożliwiać tworzenie raportów ze szczegółami wykrytych alertów do formatów co najmniej JSON, CSV.
   41. Analizator musi umożliwiać tworzenie raportów z przeprowadzonych skanowań do formatu PDF zawierających co najmniej statystyki wykrytych zagrożeń.
   42. Analizator musi umożliwiać przegląd nowych funkcjonalności po aktualizacji oprogramowania.
   43. Analizator musi umożliwiać przegląd statystyki danych zebranych na poszczególnych interfejsach urządzenia.
   44. Analizator musi umożliwiać tworzenie raportów uruchamianych cyklicznie (godzinowo/dzienne/tygodniowo/miesięcznie) zawierających co najmniej wykryte zagrożenia. Raporty te muszą być dostarczane przez email.
   45. Analizator musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły RSYSLOG, SMTP, SNMP, HTTP.
   46. Analizator musi integrować się bezpośrednio z posiadanym przez zamawiającego modułem centralnego zarządzania FireEye CM co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów,
   47. Analizator musi umożliwiać korelację alertów z MITRE Technics.
   48. Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Office 365 SharePoint Online storage.
   49. Analizator musi umożliwiać natywną integrację umożliwiającą skanowanie plików z Microsoft OneDrive.
   50. Analizator musi wspierać możliwość podłączenia repozytoriów CIFS po SMBv3.