OPIS PRZEDMIOTU ZAMÓWIENIA

ROZDZIAŁ I. OGÓLNE WARUNKI REALIZACJI ZAMÓWIENIA

1. Przedmiot zamówienia:

Przedmiotem zamówienia jest zapewnienie przez Wykonawcę na rzecz Odbiorcy dostępu do rozwiązania informatycznego obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej, ochrony dostępu do sieci Internet, platformy do analizy złośliwych plików, modułu ochrony udziałów sieciowych oraz modułu do zarządzania.

2. W ramach przedmiotu zamówienia stanowiącego zamówienie Wykonawca jest zobowiązany w szczególności do:
   1) dostawy, instalacji, konfiguracji i uruchomienia Systemu składającego się z:
      a) moduł wielopoziomowej ochrony poczty elektronicznej,
      b) moduł ochrony dostępu do sieci Internet,
      c) moduł do analizy złośliwych plików,
      d) moduł do ochrony udziałów sieciowych,
      e) moduł do zarządzania,

zgodnie ze specyfikacją techniczną opisaną w Rozdziale II,

   2) udzielenia lub zapewnienia udzielenia wszelkich licencji wymaganych do prawidłowego działania Systemu jako całości, jak i poszczególnych jego elementów dla 2000 użytkowników, na okres 36 miesięcy. Licencjobiorcą jest Odbiorca,
   3) dostarczenia Sprzętu wymaganego do prawidłowego działania Systemu,
   4) udzielenia 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,
   5) udzielenia odbiorcy Gwarancji na dostarczony w ramach Umowy Sprzęt, na okres 36 miesięcy od podpisania Protokołu Odbioru Wdrożenia Systemu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie dostarczonego Sprzętu, w ramach wynagrodzenia wynikającego z Umowy,
   6) świadczenia usług serwisu w ramach Gwarancji na System, Gwarancji na Sprzęt i wsparcia technicznego dla środowiska. Wymagania dotyczące serwisu i wsparcia technicznego zostały opisane w Rozdziale I w pkt 5, pkt 6 oraz pkt 7,
   7) wykonania dokumentacji szczegółowo opisanej w Rozdziale II w pkt 7,
   8) przeniesienia na Odbiorcę autorskich praw majątkowych do Dokumentacji opracowanej przez

Wykonawcę w ramach Umowy,

9) świadczenia w ramach prawa opcji usług asysty technicznej eksperta w liczbie do 500 roboczogodzin. Wymagania dotyczące usług asysty technicznej eksperta zostały uszczegółowione w Rozdziale I w pkt 8,
10) przeprowadzenia transferu wiedzy. Wymagania dotyczące transferu wiedzy zostały opisane w Rozdziale III w pkt 8.
11) dostarczenia w ramach prawa opcji maksymalnie 4 szt. Sprzętu Trellix FX lub równoważnego Sprzętu, o który oparty jest zaoferowany System, o parametrach tożsamych lub wyższych niż Sprzęt zaoferowany w ramach dostarczonego Systemu. Wymagania dotyczące rozbudowy zostały uszczegółowione w Rozdziale I w pkt 9,

3. Zamawiający dopuszcza zaoferowanie rozwiązania wykorzystującego aktualnie posiadaną przez Odbiorcę infrastrukturę:
   1) Moduł wielopoziomowej ochrony poczty elektronicznej

      Forcepoint ESG:

      - 4 serwery Forcepoint V10000 G4R2
      - Licencje (ważne do 26.08.2025):
        - Forcepoint Email Security
        - Forcepoint V10000 G4R2 Appliance
        - Support

      Trellix Email Gateway:

      - 2 serwery FireEye EX 3500
      - Licencje (ważne do 26.08.2025):
        - LK2-FIREEYE_APPLIANCE
        - LK2-FIREEYE_SUPPORT
        - LK2-CONTENT_UPDATES
        - LK2-EMPS_ATTACHMENT_SCAN
        - LK2-EMPS_URL_SCAN
   2) Moduł ochrony dostępu do sieci Internet:

      Forcepoint WSG

      - 4 serwery Forcepoint V10000 G4R2
      - Licencje (ważne do 26.08.2025):
        - Forcepoint Web Security
        - Forcepoint V10000 G4R2 Appliance
        - Support

3) Moduł do analizy złośliwych plików:

Trellix AX

- 1 serwerNFAX-5600G
- Licencje (ważne do 04.09.2025):
  - LK2-FIREEYE_APPLIANCE
  - LK2-FIREEYE_SUPPORT
  - LK2-CONTENT_UPDATES

4) Moduł do ochrony udziałów sieciowych:

Trellix FX:

- 1 serwer FireEye FX 6500
- Licencje (ważne do 07.09.2025):
  - LK2-FIREEYE_APPLIANCE
  - LK2-FIREEYE_SUPPORT
  - LK2-CONTENT_UPDATES

5) Moduł do zarządzania:

Forcepoint FSM

Trellix CM

- 1 serwer CM-4600G
- Licencje (ważne do 04.09.2025):
  - LK2-FIREEYE_APPLIANCE
  - LK2-FIREEYE_SUPPORT
  - LK2-CONTENT_UPDATES

z zastrzeżeniem, że Wykonawca musi w ramach zamówienia przedłużyć posiadanie licencje oraz dostarczyć jeden dodatkowy Trellix FX wraz z wymaganym licencjami na urządzenie (o ile dotyczy).

4. Wymagania w zakresie dokumentacji:
   1) Wykonawca w uzgodnieniu z Zespołem Odbiorowym opracuje i przekaże Dokumentację Projektową dla wdrożenia nowego serwera Trellix FX:
      a. Projekt Wdrożenia nowego serwera Trellix FX, który musi zawierać co najmniej: opis funkcjonalny, wykaz wymaganych elementów, sposób wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania nowego serwera Trellix FX, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia. Szczegółowe informacje dot. tej infrastruktury zostaną przekazane Wykonawcy, z którym zostanie zawarta Umowa.

b. Dokumentację Testów Akceptacyjnych dla wdrożenia nowego serwera Trellix FX, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony nowy serwer Trellix FX 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 zaktualizuje istniejącą 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 obejmującej co najmniej:
   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 musi być przekazana w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być przekazane w języku angielskim lub polskim i przekazana Odbiorcy na adres e-mail wskazany w trybie roboczym.

5. Wymagania w zakresie Gwarancji na System:
   1) Wykonawca nie później niż w terminie 10 dni od dnia zawarcia Umowy, ma obowiązek przekazać Odbiorcy w formie pisemnej dokument „Instrukcja zgłaszania, obsługi i eskalacji zgłoszeń serwisu", zawierający:
   a) instrukcje zgłaszania awarii;
   b) szczegółowy opis procedury eskalacji zawierającej co najmniej dodatkowy numer telefonu i adres e-mail (pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub braku reakcji na zgłoszenie);
   c) dane Wykonawcy - adresy, numery telefonów, adresy poczty elektronicznej;
   d) instrukcje dotyczące pobierania poprawek i nowych wersji oprogramowania ze strony internetowej dla urządzeń i oprogramowania bez ponoszenia dodatkowych kosztów;
   e) wzór Raportu z naprawy urządzenia.

   Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe procedury. Przekazane przez Wykonawcę instrukcje i procedury podlegają

akceptacji Odbiorcy. Odbiorca może zgłosić uwagi i poprawki do instrukcji i procedur przekazanych przez Wykonawcę, a Wykonawca jest zobowiązany do ich niezwłocznego uwzględnienia i przedstawienia do ponownej akceptacji przez Odbiorcę.

2) W przypadku jakichkolwiek zmian danych, o których mowa w ppkt 1) powyżej, w tym danych, o których mowa w ppkt 1) lit. c, Wykonawca niezwłocznie poinformuje o tym Odbiorcę pisemnie, co wymaga akceptacji Odbiorcy. Instrukcje, o których mowa powyżej, nie mogą być sprzeczne lub niezgodne z postanowieniami Umowy.
3) Zgłoszenie awarii będzie dokonywane poprzez:
   a) zgłoszenie telefoniczne,
   b) pocztę elektroniczną,
   c) serwis www udostępniony przez Odbiorcę.

   W przypadku dokonania zgłoszenia telefonicznego, Odbiorca potwierdzi je za pomocą poczty elektronicznej lub z wykorzystaniem serwisu www udostępnionego przez Odbiorcę.
4) Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu.
5) W ramach udzielonej Gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe Awarii Systemu w następujący sposób:
   a) **Awaria Krytyczna**, oznacza całkowite unieruchomienie Systemu lub jego kluczowych funkcjonalności, które uniemożliwiają korzystanie z Systemu przez wszystkich lub większość użytkowników. Awaria krytyczna dotyczy zarówno Oprogramowania, jak i Sprzętu. Także sytuacje, w których przerwa w działaniu Systemu może prowadzić do braku zachowania ciągłości działania instytucji Odbiorcy lub może mieć wpływ na bezpieczeństwo danych. Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 12 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;
   b) **Awaria Niekrytyczna**, oznacza nieprawidłowość działania Systemu, która powoduje ograniczenie jego funkcjonalności w sposób istotny lecz nie całkowicie uniemożliwiający jego użytkowanie. Dostępna może być część funkcji Systemu, jednak niektóre funkcje mogą działać wadliwie bądź w stopniu ograniczonym. Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;
   c) **Usterka,** wada niskiego znaczenia, która nie wpływa na pracę Systemu. Nieprawidłowość działania Systemu niskiego znaczenia nie wpływająca na jego podstawowe funkcjonalności, a jedynie na estetykę i wygodę użytkowania. Ponadto może też powodować m.in. sporadyczne błędy, które można łatwo obejść, a które nie zakłócają ciągłości działania Systemu. Czas reakcji

do 8 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę, Czas Naprawy do 10 dni roboczych od chwili Zgłoszenia Serwisowego przez Odbiorcę.

d) Odbiorca zastrzega sobie prawo do zmiany kategorii zgłoszenia w trakcie jego obsługi, jeśli jego wpływ na działanie Systemu będzie odpowiadał kryteriom wyższej kategorii. W przypadku wątpliwości dotyczących kategoryzacji zgłoszenia, decydujące znaczenie ma ocena Odbiorcy.

6) Wykonawca będzie przyjmował zgłoszenia awarii lub konsultacji technicznych w ramach serwisu i wsparcia technicznego całodobowo - 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

7) Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia zgodnie z zapisami ppkt 5) na adres poczty elektronicznej ..... lub telefonicznie – na numer podany podczas rejestracji zgłoszenia. W przypadku braku potwierdzenia zgłoszenia Awarii, po upływie czasu reakcji, zgodnie z zapisami ppkt 5), Odbiorca wdroży procedurę eskalacji zgłoszenia.

8) 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.

9) W przypadku, gdy Wykonawca nie wykona obowiązków wynikających z ppkt 5), w terminach tam wskazanych:

a) Odbiorca ma prawo wypożyczyć, zainstalować i uruchomić system zastępczy, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do żądania kary umownej i odszkodowania na zasadach ogólnych przewyższającego wysokość kary umownej;

b) Odbiorca ma prawo zlecić innemu podmiotowi naprawę Systemu, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do żądania kary umownej i odszkodowania na zasadach ogólnych przewyższającego wysokość kary umownej.

10) W okresie trwania Umowy Odbiorca ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów (np. modułów optycznych itp.) oraz rozbudowy urządzeń oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego posiadanych urządzeń (firmware), zgodnie z zasadami wiedzy technicznej przez Odbiorcę lub podmiot zewnętrzny, któremu zleci te prace Odbiorca.

11) Oferowane oprogramowanie i urządzenia, w ramach zamówienia będą pochodziły z oficjalnego kanału dystrybucyjnego na terenie Unii Europejskiej.

12) Odbiorca wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień wdrożenia Systemu.

13) Rozszerzenie licencji o kolejne funkcjonalności nie może powodować utraty praw gwarancyjnych do oprogramowania oraz nie może wymagać zgody Wykonawcy lub producenta oprogramowania.

14) Odbiorca wymaga, aby Wykonawca w ramach serwisu na wniosek Odbiorcy aktualizował firmware urządzeń.
15) Wykonawca zobowiązany jest do udzielenia Gwarancji jakości oraz rękojmi dla dostarczonych urządzeń i licencji.
16) Okres wsparcia oraz Gwarancji i rękojmi na System nie będzie krótszy niż okres obowiązywania Umowy.

6. Wymagania w zakresie wsparcia technicznego na System:

1) Wykonawca zapewni wsparcie techniczne dla całego Systemu, w tym oprogramowania i licencji.
2) Wsparcie techniczne musi obejmować co najmniej:
   a) aktualizację i konfigurację oprogramowania przez Wykonawcę,
   b) rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem, konfiguracją i obsługą Systemu,
   c) instalację przez Wykonawcę nowych wersji oprogramowania systemu, poprawek i usprawnień udostępnionych przez producenta, dokonywaną na wezwanie i w terminie uzgodnionym z Odbiorcą.
3) W ramach udzielonego wsparcia technicznego 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.
4) Zamawiający wymaga, aby w ramach wsparcia technicznego Wykonawca zapewnił:

a) dostęp do portali internetowych zawierających narzędzia wsparcia elektronicznego urządzeń i oprogramowania stanowiącego przedmiot Umowy oraz zapewni możliwość korzystania z nich przez cały okres obowiązywania Umowy,
b) pobieranie z serwera WWW lub FTP poprawek i aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego urządzeń (firmware) stanowiących przedmiot Umowy, umożliwiających jego instalację, udostępnionych w okresie trwania Umowy; pobieranie tych aktualizacji musi być zgodne z zasadami licencjonowania producenta oprogramowania,

5) Konsultacje techniczne w ramach wsparcia technicznego mogą być przeprowadzone pomiędzy Wykonawcą a Odbiorcą osobiście, telefonicznie lub za pomocą poczty elektronicznej,
6) Odbiorca w ramach serwisu i wsparcia technicznego musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną do Wykonawcy, bez ograniczeń, co do liczby zgłoszeń.

7. Wymagania w zakresie Gwarancji na Sprzęt:

Świadczenia gwarancyjne w zakresie Sprzętu realizowane będą z uwzględnieniem następujących zasad:

1) usługi gwarancyjne będą świadczone przez producenta Sprzętu lub podmiot posiadający autoryzację producenta Sprzętu, w miejscu użytkowania Sprzętu, jeśli jednak naprawa Sprzętu w tym miejscu okaże się niemożliwa, naprawa może zostać wykonana w innym miejscu; usługi gwarancyjne Sprzętu będą świadczone w Dni Robocze, w godzinach od 8:00 do 16:00;
2) w zakres usług gwarancyjnych wchodzi również dojazd i praca osób wykonujących czynności gwarancyjne w imieniu Wykonawcy oraz pozostałe koszty niezbędne do świadczenia usług gwarancyjnych, w tym koszty dostawy i odbioru wymienionych urządzeń, niezależnie od podmiotu wykonującego usługę gwarancyjną;
3) na czas naprawy Sprzętu poza miejscem jego użytkowania Sprzęt zabierany będzie bez dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy). Po zwrocie naprawionego Sprzętu dysk twardy lub inne elektroniczne nośniki informacji zostaną ponownie zamontowane przez Wykonawcę, po czym nastąpi sprawdzenie poprawności funkcjonowania naprawionego Sprzętu;
4) w przypadku nieodwracalnej awarii dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy) będą one wymienione przez Wykonawcę na nowy, wolny od wad fizycznych i prawnych, o parametrach nie gorszych niż te, które uległy awarii. Uszkodzony dysk twardy lub inne elektroniczne nośniki informacji nie będzie podlegał zwrotowi Wykonawcy. Koszty dysków twardych wymienianych z powodu ich awarii ponosi Wykonawca;
5) Wykonawca zobowiązuje się zapewnić, że każda osoba wykonująca usługi gwarancyjne w miejscu wykorzystywania Sprzętu, będzie posiadała dokument tożsamości i pisemne upoważnienie do wykonywania napraw i czynności objętych Gwarancją, potwierdzone przez Wykonawcę oraz będzie zobligowana stosować się do przepisów wewnętrznych Odbiorcy dotyczących ruchu osobowego i materiałowego w jego siedzibie;
6) Usługi gwarancyjne wykonywane będą przy wykorzystaniu materiałów, sprzętu i narzędzi Wykonawcy, chyba że naprawa zostanie wykonana w punkcie serwisowym producenta nie będącego Wykonawcą;
7) Części lub podzespoły, które zostaną wymienione w ramach usług gwarancyjnych stają się własnością Wykonawcy, który zobowiązuje się do ich bezpośredniego odbioru od Odbiorcy i utylizacji zgodnie z obowiązującymi przepisami;
8) W przypadku wymiany części lub podzespołów, Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną dla wymienionych elementów Sprzętu, (jeżeli ich producent udziela odrębnej Gwarancji);

9) W przypadku Awarii Sprzętu i konieczności naprawy Sprzętu, Wykonawca zobowiązany jest do dostarczenia najpóźniej w następnym dniu roboczym od dnia zgłoszenia, na swój koszt, do siedziby Odbiorcy, Sprzętu zastępczego o parametrach nie gorszych niż Sprzęt, który podlega naprawie, na cały okres naprawy Sprzętu, posiadającego stosowne certyfikaty/ dokumenty;
10) W razie niedokonania naprawy Sprzętu (usunięcia awarii) w terminie: dopuszcza się dokonanie naprawy siłami własnymi Odbiorcy na koszt Wykonawcy lub zlecenie naprawy osobie trzeciej na koszt Wykonawcy, z zachowaniem praw wynikających z Gwarancji i rękojmi za wady Sprzętu, bez dodatkowego wezwania Wykonawcy do wykonania usługi gwarancyjnej. W przypadku skorzystania z powyższego uprawnienia, Wykonawca zostanie niezwłocznie powiadomiony w formie pisemnej o tym fakcie oraz zakresie zleconych prac (napraw, zmian, itp.). W takim przypadku Wykonawca zobowiązany jest zapłacić Odbiorcy – w terminie przez Niego wskazanym, nie krótszym jednak niż 14 dni kalendarzowych – kwotę stanowiącą równowartość poniesionego przez Odbiorcę kosztu wykonania tych prac;
11) Okres Gwarancji przedłuża się o czas trwania naprawy;
12) Rozbudowa lub modyfikacje Sprzętu nie mogą prowadzić do utraty uprawnień wynikających z rękojmi za wady urządzenia lub utraty prawa do korzystania z usług gwarancyjnych;
13) W ramach usunięcia awarii Odbiorca dopuszcza możliwość wymiany przez Wykonawcę, po uzgodnieniu z Odbiorcą, poszczególnych elementów lub podzespołów urządzenia lub całego urządzenia na fabrycznie nowe, wolne od wad fizycznych i prawnych, takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie. Postanowienie ppkt 12 stosuje się odpowiednio;
14) W przypadku, gdy w wyniku usuwania awarii Wykonawca zapewnił urządzenie zastępcze, a naprawa urządzenia trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/część urządzenia będzie podlegać naprawie trzykrotnie w okresie obowiązywania Umowy, Wykonawca zobowiązany jest dokonać wymiany elementu/podzespołu/części urządzenia na nowy, o takich samych lub lepszych funkcjonalnościach oraz takich samych lub lepszych parametrach, bez dodatkowego wezwania Wykonawcy. Wymiana Sprzętu na nowy powinna zostać potwierdzona protokołem, który zawierał będzie co najmniej datę dostawy nowego Sprzętu. W takiej sytuacji termin Gwarancji biegnie na nowo od chwili dostarczenia i potwierdzenia protokolarnego dostawy nowego Sprzętu. Dostarczone w ramach wymiany urządzenie musi być wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą, wolne od wad fizycznych i prawnych, fabrycznie nowe - bez śladów używania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczypospolitej Polskiej i dostarczone Odbiorcy w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. W przypadku wymiany urządzenia na nowe, Wykonawca sporządzi protokół

z wymiany urządzenia dostarczonego w ramach wymiany - Protokół Wymiany Sprzętu. Z chwilą podpisania protokołu na Odbiorcę przechodzi prawo własności nowego urządzenia;

15) Wykonawca każdorazowo dostarczy Odbiorcy Raport z naprawy urządzenia, zawierający datę i godzinę zgłoszenia, przystąpienia do realizacji zgłoszenia, datę i godzinę usunięcia awarii, informację co było przedmiotem naprawy. Raporty z naprawy urządzenia będą przygotowywane przez Wykonawcę w języku polskim i przesłane na adres poczty elektronicznej Odbiorcy. Odbiorca w terminie 3 dni roboczych od otrzymania Raportu z naprawy urządzenia dokonuje jego akceptacji lub zgłasza do niego uwagi, przesyłając je na adres poczty elektronicznej Wykonawcy. Wykonawca zobowiązany jest w terminie 2 dni roboczych od dnia otrzymania uwag do ich uwzględniania i przedstawienia poprawionej wersji Raportu z naprawy urządzenia, a w razie nieuwzględnienia uwag – do pisemnego uzasadnienia swojego stanowiska. W takim przypadku stosuje się postanowienie zdania poprzedniego.

8. Asysta techniczna eksperta – wymagania **(opcjonalny zakres zamówienia)**
   1) Świadczenie Usługi Asysty Technicznej jest uprawnieniem Odbiorcy i stanowi opcjonalny zakres zamówienia. Niewykorzystanie w całości lub w jakiejkolwiek części przewidzianych w Umowie roboczogodzin, nie rodzi po stronie Wykonawcy żadnych roszczeń z tego tytułu w stosunku do Zamawiającego lub Odbiorcy.
   2) Wykonawca będzie świadczyć usługi asysty technicznej eksperta rozumianego jako certyfikowanego przez producenta inżyniera systemowego dla całości rozwiązania wdrożonego przez Wykonawcę do końca trwania Umowy od dnia podpisania przez Odbiorcę bez zastrzeżeń Protokołu Odbioru Wdrożenia Systemu lub do wyczerpania puli roboczogodzin usług asysty technicznej eksperta, w zależności, które zdarzenie nastąpi wcześniej, usługi świadczone w języku polskim;
   3) W roboczogodzinę usługi asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie, tzn. nie ma znaczenia, ile osób będzie świadczyło usługę asysty technicznej eksperta w danej roboczogodzinie/roboczogodzinach u Odbiorcy. Rozliczenie roboczogodzin usług asysty technicznej eksperta odbywać się będzie miesięcznie za faktycznie wykorzystane roboczogodziny na podstawie Protokołów Odbioru Usług Asysty Technicznej Eksperta. Do roboczogodzin usługi asysty technicznej eksperta nie wlicza się godzin usług wykonywanych w ramach Gwarancji lub rękojmi oraz serwisu;
   4) Zakres czynności wykonywanych w ramach usług asysty technicznej eksperta nie może być tożsamy z zakresem objętym serwisem i wsparciem technicznym. W przypadku, gdy Odbiorca zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu i wsparcia technicznego, Wykonawca ma obowiązek poinformowania o tym fakcie Odbiorcę. Natomiast

w przypadku sytuacji odwrotnej, gdy Odbiorca zleci Wykonawcy prace, które powinny być zrealizowane w ramach usług asysty technicznej eksperta i tak Wykonawca to liczy, to ma obowiązek poinformowania o tym fakcie Odbiorcę;

5) Zlecenia w ramach usługi asysty technicznej eksperta, zgłaszane przez Odbiorcę, będą dotyczyły w szczególności:
    a) rozwoju i modyfikacji Sprzętu i rozbudowa Systemu,
    b) zaawansowanej konfiguracji Sprzętu i Systemu,
    c) wsparcia w zakresie utrzymania Sprzętu i Systemu (m.in. np. migracje, integracje i testowanie komponentów środowiska),
    d) optymalizację parametrów działania Systemu,
    e) analizy i audyty środowiska,
    f) wsparcia merytorycznego oraz transferu wiedzy,
    g) przygotowanie dokumentacji technicznej, procedur, instrukcji,
    h) inne niestandardowe wsparcie wymagające udziału eksperta;
6) Osoby uprawnione w Umowie przez Odbiorcę będą każdorazowo przekazywać Wykonawcy zlecenia w ramach usługi asysty technicznej eksperta, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia oraz miejsce realizacji;
7) Wykonawca w terminie wyznaczonym przez Odbiorcę, nie krótszym niż 2 dni robocze od otrzymania zlecenia, przekaże Odbiorcy propozycję wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, tj. proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia wraz z rozbiciem na poszczególne czynności;
8) Odbiorca może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia;
9) Odbiorca zastrzega sobie prawo do zakwestionowania zaproponowanego przez Wykonawcę terminu realizacji oraz wyceny zleconych prac. W takiej sytuacji, Strony w drodze uzgodnień doprowadzą do akceptowalnej wyceny zleconych prac oraz terminu ich realizacji, co zostanie potwierdzone pisemnie, poprzez aktualizację zlecenia Asysty Technicznej.
10) Odbiorca zastrzega sobie prawo do ostatecznego odrzucenia propozycji Wykonawcy i rezygnacji z realizacji zleconych prac, bez ponoszenia kosztów opisu sposobu wykonania zlecenia i przygotowania wyceny przez Wykonawcę.
11) W przypadku akceptacji propozycji sposobu wykonania zlecenia, Odbiorca przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę

roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac. Zatwierdzone przez Odbiorcę zlecenie Usług Asysty Technicznej jest równoznaczne ze złożeniem oświadczenia w zakresie uruchomienia opcjonalnego zakresu zamówienia.

12) Rozliczenie Usługi Asysty Technicznej odbywać się będzie każdorazowo na podstawie podpisanego bez zastrzeżeń przez Odbiorcę, Protokołu Odbioru Usług.
13) Odbiorca może wyrazić zgodę na wykonanie zlecenia zdalnie, w takim przypadku Wykonawca zobowiązany jest do przestrzegania wszystkich wymagań Odbiorcy. Odbiorca zastrzega sobie prawo do odmowy, przerwania świadczenia usługi zdalnego dostępu w dowolnym momencie bez wcześniejszego informowania Wykonawcy.

9. Dodatkowy sprzęt – wymagania (opcjonalny zakres zamówienia)

1) Odbiorca zastrzega sobie możliwość rozbudowy Systemu o maksymalnie 4 szt. Sprzętu Trellix FX lub równoważnego lub Sprzętu, o który oparty jest zaoferowany System, o parametrach tożsamych lub wyższych niż Sprzęt zaoferowany w ramach dostarczonego Systemu.
2) Dostarczenie dodatkowego Sprzętu jest uprawnieniem Odbiorcy i stanowi opcjonalny zakres zamówienia. Niewykorzystanie w całości lub w jakiejkolwiek części przewidzianych w Umowie maksymalnej ilości Sprzętu nie rodzi po stronie Wykonawcy żadnych roszczeń z tego tytułu w stosunku do Zamawiającego lub Odbiorcy.
3) Dostarczenie dodatkowego Sprzętu polegać będzie na:
   a) dostawie Sprzętu w miejsce wskazane przez Odbiorcę
   b) instalacji i konfiguracji dostarczonego Systemu z uwzględnieniem istniejącej infrastruktury Systemu
   c) udzielenia odbiorcy Gwarancji na dostarczony w ramach Umowy Sprzęt, na okres 36 miesięcy od podpisania Protokołu Odbioru Sprzętu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie dostarczonego Sprzętu, w ramach wynagrodzenia wynikającego z Umowy
   d) świadczenia usług serwisu w ramach Gwarancji na Sprzęt. Wymagania dotyczące serwisu i wsparcia technicznego zostały opisane w Rozdziale I w pkt 5, pkt 6 oraz pkt 7,
   e) wykonania dokumentacji szczegółowo opisanej w Rozdziale II w pkt 7,
   f) przeniesienia na Odbiorcę autorskich praw majątkowych do Dokumentacji opracowanej przez Wykonawcę w ramach zamówienia opcjonalnego.
4) Osoby uprawnione w Umowie przez Odbiorcę będą przekazywać Wykonawcy zlecenia dostawy Sprzętu, w których określona zostanie ilość Sprzętu, maksymalny termin realizacji zlecenia, miejsce realizacji zlecenia, kwotę wynagrodzenia należnego za zrealizowanie zlecenia wyliczoną w oparciu o ceny jednostkowe wskazane w ofercie złożonej w postępowaniu o udzielenie zamówienia

5) Przekazanie zlecenia jest równoznaczne ze złożeniem oświadczenia w zakresie uruchomienia opcjonalnego zakresu zamówienia.
6) Rozliczenie dostaw dodatkowego Sprzętu odbywać się będzie każdorazowo na podstawie podpisanego bez zastrzeżeń przez Odbiorcę, Protokołu Odbioru Dostaw Sprzętu.

ROZDZIAŁ II. WYMAGANIA DLA OFERTY

1. Wymagania ogólne:
   1.1. Oferowany System musi obejmować kompleksowe rozwiązanie gwarantujące ochronę przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising), złośliwym oprogramowaniem (malware) oraz ochronę dostępu do sieci Internet, wraz z narzędziami do wykrywania infekcji, po włamaniowej mitygacji i analizy zagrożeń. Ochrona przed złośliwym oprogramowaniem w poczcie email musi być realizowana w oparciu o tradycyjne bazy sygnatur jak i również poprzez uruchamianie podejrzanego kodu w izolowanych środowiskach maszyn wirtualnych (sandbox). Kontrola dostępu do sieci Internet musi być zrealizowana przez rozwiązanie klasy Proxy (Web Gateway).
   1.2. System musi składać się z minimum z trzech Modułów. W celu zapewnienia wielopoziomowej ochrony poczty elektronicznej i zwiększając szansę wykrycia niebezpiecznych wiadomości email wymagane jest dostarczenie rozwiązań ochrony poczty dwóch niezależnych Producentów. Moduł Proxy ma realizować weryfikację dostępu do sieci Internet wraz z zawansowaną analizą adresów URL.
   1.3. Zadaniem pierwszego Modułu (Moduł AntySpam) musi być zaawansowana ochrona poczty elektronicznej przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising) oraz złośliwym oprogramowaniem.
   1.4. 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).
   1.5. Uruchamianie podejrzanego kodu (załączników, obiektów) w izolowanych środowiskach maszyn wirtualnych musi odbywać się lokalnie, bez wysyłania analizowanych elementów poza siedzibę Odbiorcy.
   1.6. Zadaniem trzeciego Modułu (Moduł Proxy) musi być zaawansowana ochrona dostępu do sieci Internet. Moduł musi zapewniać funkcję filtrowania URL, analizę oraz kategoryzację stron, inspekcję i zarządzanie szyfrowanymi połączeniami HTTPS wraz z pełną inspekcją szyfrowanego ruchu (posiada wbudowaną funkcjonalność deszyfrowania ruchu HTTPS),

ochronę przeciwko atakom malware wykorzystując statyczne sygnatury jak i złożoną ocenę ryzyka i predykcyjną analizę. W szczególności moduł ma dodatkowo chronić przez niebezpiecznymi URL'ami które mogły przedostać się w poczcie email.

1.7. Dostarczone rozwiązania dla modułu wielopoziomowej ochrony poczty elektronicznej oraz modułu ochrony dostępu do sieci Internet musi zapewniać odpowiednią ilość sprzętu dla zapewnienia pracy w dwóch ośrodkach przetwarzania danych, podstawowym i zapasowym, działające w trybie Active-Active (wysoka dostępność i równoważenie obciążenia). Każde urządzenie powinno umożliwiać rozbudowę (tzw. scale-up lub scale-out).

1.8. Dostarczenie rozwiązania do ochrony udziałów sieciowych w oparciu o urządzenia/appliance Trellix FX (lub równoważne), zapewniające pełną ochronę ruchu sieciowego. Rozwiązanie musi zostać zrealizowane w oparciu o co najmniej dwa niezależne urządzenia FX (lub równoważne) zainstalowane w dwóch ośrodkach przetwarzania danych, działające w trybie Active-Active (wysoka dostępność i równoważenie obciążenia). Każde urządzenie musi umożliwiać rozbudowę (tzw. scale-up lub scale-out).

1.9. 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.

1.10. 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.

1.11. W celu ograniczenia ilości konsol zarządzających, Moduły AntySpam oraz Moduł Proxy muszą pochodzić od jednego producenta.

1.12. Oferowany System składać się musi z minimum trzech Modułów i będzie pochodził tylko z oficjalnych kanałów dystrybucyjnych Producentów Modułów na terenie Unii Europejskiej.

1.13. 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.

1.14. 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.

1.15. Wymaganiem Zamawiającego jest, aby każdy Moduł posiadał tylko jedną konsolę zarządzającą.

1.16. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).

1.17. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).

1.18. Zamawiający wymaga, aby wszystkie elementy i Moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu.

1.19. Żaden z Modułów i elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.

1.20. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Odbiorcy Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Odbiorcy.

2. Moduł wielopoziomowej ochrony poczty elektronicznej:

1. Wymagania funkcjonalne i techniczne dla Modułu AntySpam:

1.1. Moduł AntySpam musi realizować funkcje ochrony przed spamem i zagrożeniami bezpieczeństwa w ruchu SMTP.

1.2. Moduł AntySpam musi umożliwiać filtrowanie poczty zarówno przychodzącej, wychodzącej jak i komunikacji wewnętrznej między różnymi domenami, dlatego musi być możliwość definiowania osobnych zestawów polityk dla każdego z kierunków przesyłania wiadomości.

1.3. Moduł AntySpam musi realizować następujące funkcje bezpieczeństwa poczty elektronicznej:

1.3.1. kontrola protokołu SMTP z uwzględnieniem jego szyfrowanych wersji SSL i TLS,

1.3.2. ochrona przed spamem,

1.3.3. ochrona przed szkodliwą zawartością (wirusy, malware, itp.),

1.3.4. ochrona przed niebezpiecznymi odnośnikami URL w treści wiadomości,

1.4. Architektura Modułu AntySpam musi składać się z:

1.4.1. Centralnego serwera zarządzania Modułu AntySpam, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa poczty elektronicznej i raportowania oraz

1.4.2. Bram (ang. Gateway) służących do egzekwowania polityk bezpieczeństwa poczty elektronicznej oraz przesyłanych danych i pracujących w trybie MTA (ang. Mail Transfer Agent).

1.5. Centralny serwer zarządzania i raportowania musi być dostarczony w postaci oprogramowania, którego instalacja musi być możliwa minimum w następujących systemach operacyjnych: Microsoft Windows Server 2016 lub Microsoft Windows Server 2019.

1.6. Centralny serwer zarządzania musi umożliwiać logowanie użytkowników do Modułu z wykorzystaniem kont lub grup użytkowników z usługi katalogowej, np. Microsoft Active Directory.

1.7. Centralny serwer zarządzania musi umożliwiać konfigurację uprawnień dla administratorów systemu na podstawie skonfigurowanych ról. Role muszą pozwalać przynajmniej na konfigurację następujących poziomów dostępu:

1.7.1. Brak dostępu do wybranej funkcji systemu.

1.7.2. Dostęp tylko do odczytu.

1.7.3. Pełny dostęp.

1.8. Centralny serwer zarządzania modułu AntySpam musi posiadać wspólną konsolę do zarządzania z modułem Proxy (ochrona dostępu do sieci Internet) oraz opcjonalnym modułem do ochrony danych wrażliwych (DLP), dostarczanymi od tego samego producenta.

1.9. Integracja z usługą katalogową musi dodatkowo umożliwiać konfigurację następujących ograniczeń dostępu do centralnej konsoli podczas definiowania roli:

1.9.1. Dostępu do raportów z danych pochodzących tylko od użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.

1.9.2. Dostęp do logów wiadomości przesyłanych tylko od i do użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.

1.9.3. Dostęp do wybranych kolejek wiadomości należących tylko do użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.

1.9.4. Zarządzanie politykami przypisanymi tylko do grupy użytkowników należących do wybranej grupy użytkowników z usługi katalogowej.

1.10. 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.

1.11. System musi składać się z przynajmniej czterech serwerów Gateway (Bram pocztowych). Po dwa w każdej lokalizacji, pracujące w trybie wysokiej dostępności niezależnie dla każdej z lokalizacji, które muszą być dostarczone w postaci:

1.11.1. Rozwiązania sprzętowego na dedykowanej platformie dostarczanej przez tego samego producenta w formie urządzenia do montażu w rack o następujących minimalnych wymaganiach sprzętowych:

1.11.1.1. Dwa procesory Intel Xeon Silver seria 4000,

1.11.1.2. Pamięć RAM 32 GB,

1.11.1.3. Dwa zasilacze 700W, wymienne w trakcie pracy (Hot Swappable),

1.11.1.4. Cztery interfejsy sieciowe RJ-45 w standardzie Ethernet 1GbE oraz dwa porty SFP z możliwością zamontowania wkładek 10Gbe i 1Gbe,

1.11.1.5. Trzy dyski twarde o pojemności 300GB z obsługą RAID-5 wymienne w trakcie pracy (Hot Swappable),

1.11.1.6. Wysokość urządzenia 1U w szafie Rack,

1.11.1.7. Moduł zdalnego zarządzania serwerem z dostępem do wirtualnej konsoli serwera.

1.11.2. Dostarczone przez producenta rozwiązanie musi umożliwiać także instalację dodatkowej bramy pocztowej w postaci maszyny wirtualnej gotowej do importu do środowiska wirtualnego Vmware, w postaci OVA Template, zawierającego predefiniowany dedykowany obraz systemu wytworzonego przez Producenta.

1.11.3.

1.12. Brama (Gateway) musi umożliwiać konfigurację adresów IP na różnych interfejsach sieciowych. Minimalna liczba adresowalnych interfejsów sieciowych nie może być mniejsza niż trzy.

1.13. Moduł AntySpam musi pozwalać na adresację interfejsów sieciowych z zachowaniem segmentacji, co oznacza że systemu musi pozwalać na następującą adresację:

1.13.1. Adres w sieci zarządzania, interfejs sieciowy odseparowany od pozostałych sieci,

1.13.2. Adres w sieci z dostępem do Internetu np. DMZ-Zewnętrzny, interfejs sieciowy odseparowany od pozostałych sieci,

1.13.3. Adres z sieci wewnętrznej, np. DMZ-Wewnętrzny, wykorzystywany do komunikacji z usługami wewnątrz infrastruktury, np. serwery poczty.

1.14. Segmentacja sieci Modułu AntySpam musi wykorzystywać dedykowane interfejsy sieciowe. Nie jest dopuszczalna segmentacja wykorzystująca wirtualne sieci VLAN.

1.15. Moduł AntySpam musi umożliwiać wdrożenie bram w konfiguracji wysoce dostępnego klastra active-active. Moduł musi pozwalać na użycie przynajmniej 8 bram w klastrze.

1.16. Bramy modułu muszą działać w postaci klastra nadmiarowego. Klaster odporny na awarie musi być dostarczony w jednej lokalizacji (fizyczna lokalizacja; dwa urządzenia w lokalizacji dla całego Modułu), sumarycznie minimum 2 bramy.

1.17. 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.

2. Funkcje bezpieczeństwa ochrony poczty elektronicznej Modułu AntySpam

2.1. Moduł AntySpam musi umożliwiać wykorzystanie co najmniej dwóch funkcjonalności badania reputacji nadawców dla poczty przychodzącej. Minimalne wymagania to:

2.1.1. Serwis Real-Time Blacklist (RBL) Spamhaus Datafeed dostarczony bez żadnych ograniczeń.

2.1.2. Mechanizm, który oznacza jako spam tych z nadawców, dla których odsetek spamu w wiadomościach przekroczył jeden ze zdefiniowanych poziomów.

2.2. 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:

2.2.1. braku rekordu PTR,

2.2.2. niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,

2.2.3. niezgodności rekordu PTR z rekordem A.

2.3. Moduł AntySpam musi umożliwiać weryfikację czy nadawca jest autoryzowany do wysyłania wiadomości z określonym polem nadawcy w oparciu o SPF (Sender Policy Framework).

2.4. 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:

2.4.1. nie istnieje,

2.4.2. występuje tymczasowy lub permanentny błąd, np. rekord SPF ma błędny format,

2.4.3. nie określa, czy host nadający jest autoryzowany do wysyłania maili z tej domeny,

2.4.4. zezwala hostowi nadającemu na wysyłanie maili z tej domeny, aczkolwiek host nie jest tam wprost wymieniony,

2.4.5. nie zezwala hostowi nadającemu na wysyłanie maili z tej domeny.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. Weryfikacja sygnatury DKIM w wiadomościach odbieranych przez bramkę Modułu musi być włączana osobno dla każdego z trzech kierunków przesyłania wiadomości:

2.8.1. Wiadomości przychodzące

2.8.2. Wiadomości wychodzące

2.8.3. Wiadomości wewnętrzne (dla różnych domen)

2.9. 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:

2.9.1. Algorytmy podpisywania RSA-SHA-1 lub RSA-SHA-256,

2.9.2. Możliwość podpisywania następujących nagłówków wiadomości: From, Reply-To, Subject, Date, To, Cc.

2.9.3. Możliwość podpisywania własnych nagłówków wiadomości.

2.9.4. Możliwość podpisywania treści wiadomości (ang. Body) bez limitu rozmiaru wiadomości albo z ustaleniem jaki rozmiar wiadomości zostanie podpisany.

2.10. Moduł AntySpam musi wspierać mechanizm DMARK (Domain-based Message Authentication, Reporting and Conformance) z możliwością aktywacji dla każdego z trzech kierunków przesyłania wiadomości osobno:

2.10.1. Wiadomości przychodzące

2.10.2. Wiadomości wychodzące

2.10.3. Wiadomości wewnętrzne (dla różnych domen)

2.11. 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:

2.11.1. analizę elementów wiadomości takich jak nagłówki i nadawca na kopercie wiadomości,

2.11.2. uwzględnienie wyników działania mechanizmów weryfikacji SPF, DKIM oraz SIDV (Sender ID Validation).

2.12. W ramach weryfikowania nadawcy wiadomości poprzez analizę elementów wiadomości takich jak nagłówki i nadawca na kopercie Moduł musi co najmniej porównywać czy:

2.12.1. adres nadawcy z nagłówka From: odpowiada adresowi nadawcy na kopercie wiadomości,

2.12.2. adres nadawcy z nagłówka From: odpowiada adresowi z nagłówka Reply-To,

2.12.3. adres nadawcy na kopercie wiadomości odpowiada adresowi z nagłówka Reply-To.

2.13. Moduł AntySpam bezpieczeństwa poczty musi oferować także warstwę ochrony przed oprogramowaniem złośliwym i musi opierać się o zbiór technologii automatycznie i regularnie aktualizowanych przez Producenta. Zakres tych metod musi co najmniej obejmować:

2.13.1. komercyjny silnik ochrony przed oprogramowaniem złośliwym, automatycznie i regularnie aktualizowany przez jego producenta,

2.13.2. dodatkowe metody filtracji oparte o sygnatury pochodzące z innych źródeł niż wymieniony silnik ochrony przed oprogramowaniem złośliwym,

2.13.3. metody oparte o język Yara.

2.14. 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:

2.14.1. reguły oparte o sygnatury spamu,

2.14.2. reguły leksykograficzne,

2.14.3. reguły heurystyczne.

2.15. Moduł AntySpam musi posiadać wbudowany mechanizm wykrywania wiadomości komercyjnych typu „Newsletter” i umożliwiać traktowanie tych wiadomości w zależności od ustalonej przez administratora Systemu polityki.

2.16. Moduł AntySpam musi zapewnić analizę załączników wiadomości w celu wykrycia ich rzeczywistego typu lub rozszerzenia.

2.17. Rozpoznanie typu pliku musi odbywać się w oparciu o dostarczoną przez producenta Systemu i automatycznie aktualizowaną bazę zawierającą nie mniej niż 400 typów plików.

2.18. Moduł AntySpam musi zapewnić analizę odnośników zawartych w treści oraz załącznikach wiadomości w celu zweryfikowania kategorii stron internetowych do których prowadzą.

2.19. 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:

2.19.1. Dostęp do centrum repozytorium URL Producenta, aktualizowany bezpośrednio z Modułu

2.19.2. Dostęp do lokalnego repozytorium wraz z własnymi kategoriami,

2.20. W przypadku wystąpienia w przetwarzanej wiadomości odnośnika prowadzącego do strony z wskazanych przez administratora kategorii stron internetowych system musi umożliwiać:

2.20.1. Usunięcie odnośnika z treści / tematu wiadomości

2.20.2. Modyfikację odnośnika mająca na celu jego dezaktywację

2.20.3. Zastąpienie odnośnika predefiniowanym tekstem z możliwością wykorzystania elementów dynamicznych.

2.21. Moduł AnySpam musi oferować wbudowany moduł kwarantanny.

2.22. 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.

2.23. 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.

2.24. Dodatkowo, decyzją administratora użytkownicy muszą mieć możliwość zarządzać swoimi własnymi listami zabronionych i dopuszczonych nadawców.

3. Definiowanie polityk Modułu AntySpam bezpieczeństwa poczty
   3.1. Funkcjonalność zarządzania politykami Modułu AntySpam musi umożliwiać jednokrotne definiowanie elementów takich jak filtry i akcje a następne ich wielokrotne wykorzystywanie w politykach regułach.
   3.2. Możliwe do podjęcia w ramach polityk akcje muszą obejmować co najmniej:
      3.2.1. dostarczenie wiadomości z wykonaniem dodatkowych akcji:
         3.2.1.1. zmodyfikowanie tematu wiadomości,
         3.2.1.2. usunięcie i/lub dodanie nagłówka X-header,
         3.2.1.3. wysłanie kopii wiadomości pod wskazany adres lub adresy email,
      3.2.2. zablokowanie wiadomości (kwarantanna),
      3.2.3. zapisanie wiadomości do wskazanej kolejki,
      3.2.4. wysłanie powiadomienia, gdzie:
         3.2.4.1. jego nadawcą może być oryginalny nadawca, administrator lub wskazany adres
         3.2.4.2. jego odbiorcą może być oryginalny nadawca, oryginalny adresat, administrator, wskazany adresat lub adresaci (wszyscy z wymienionych lub dowolnie wybrani)
         3.2.4.3. temat i zawartość powiadomienia mogą być w pełni dostosowane do potrzeb,
         3.2.4.4. do powiadomienia może być dołączona oryginalna wiadomość przed lub po filtrowaniu.
   3.3. 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.
   3.4. Moduł AntySpam musi zawierać predefiniowane reguły co najmniej następującego typu:
      3.4.1. Ochrona antywirus / antymalware
      3.4.2. Wykrywanie typów załączników
      3.4.3. Antyspoofing
      3.4.4. Analiza odnośników
      3.4.5. Antyspam
      3.4.6. Rozpoznawanie wiadomości komercyjnych
      3.4.7. Umieszczanie informacji / zastrzeżeń w stopce lub nagłówku wiadomości

4. Zarządzanie i raportowanie Modułu AntySpam

4.1. 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.

4.2. Moduł AntySpam musi posiadać funkcjonalność zarządzania bramami, zarówno serwerami sprzętowymi jak i maszynami wirtualnymi, uruchomiony na centralnym serwerze zarządzania.

4.3. Centralny serwerem zarządzania, musi być obsługiwany przez przeglądarkę internetową oraz musi posiadać minimum następujące funkcje:

4.3.1. Dostęp do stanu usług oraz stanu obciążenia wybranej bramy.

4.3.2. Konfigurację adresów IP dla poszczególnych interfejsów bramy.

4.3.3. Konfigurację adresów DNS wykorzystywanych przez poszczególne moduły bramy.

4.3.4. Konfigurację tras routingu.

4.3.5. Konfigurację kopii zapasowych.

4.3.6. Konfigurację powiadomień SNMP.

4.3.7. 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.

4.4. Dostęp do webowej konsoli centralnego zarządzania musi odbywać się w bezpiecznym połączeniu https.

4.5. Dostęp do konsoli centralnego zarządzania bramą musi być możliwy za pośrednictwem protokołu SSH i/lub w bezpiecznym połączeniu https.

4.6. Konsola musi wspierać silne uwierzytelnianie łączących się do niej administratorów z wykorzystaniem cyfrowych certyfikatów X.509.

4.7. 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.

4.8. Centralne zarządzanie Modułu AntySpam musi być wyposażone w funkcjonalność raportującą umożliwiającą:

4.8.1. Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem.

4.8.2. 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.

4.8.3. 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.

4.8.4. Musi być możliwe dostarczanie raportów w postaci plików pdf, xls oraz html.

4.8.5. Musi być możliwe dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.

4.9. Centralne zarządzanie musi umożliwiać delegowanie uprawnień do zarządzania i raportowania zarówno dla użytkowników domenowych jak i użytkowników tworzonych lokalnie w Systemie.

4.10. Główny administrator Moduł AntySpam musi mieć możliwość wglądu w szczegółowy audyt aktywności pozostałych administratorów zawierający następujące informacje:

4.10.1. Data akcji,

4.10.2. Nazwa administratora, który przeprowadził akcję

4.10.3. Element, na którym podejmowana jest akcja,

4.10.4. Akcja (np. zalogowanie, wylogowanie, oraz dodanie, zmiana i usunięcie obiektu),

4.10.5. W przypadku zmiany obiektu jego poprzednia i obecna wartość.

5. Integracje Modułu AntySpam

5.1. Moduł musi umożliwiać integrację z usługami katalogowymi. W tym zakresie wspierane muszą być co najmniej:

5.1.1. Microsoft Active Directory

5.1.2. LDAP Server

5.1.3. Import listy użytkowników z odpowiednio sformatowanego pliku

5.2. Moduł musi zapewnić wykorzystanie integracji z usługami katalogowymi w co najmniej następujących celach:

5.2.1. Weryfikacja adresów pocztowych odbiorców poczty przychodzącej

5.2.2. Uwierzytelnienie nadawcy poczty wychodzącej

5.2.3. Uwierzytelnienie użytkownika przy dostępnie do portalu kwarantanny

5.2.4. Weryfikacja list dystrybucyjnych

5.2.5. Kierowanie wiadomości przychodzących (ang. mail routing) w oparciu o przynależność adresata do grup użytkowników w usłudze katalogowej.

5.3. Moduł musi mieć możliwość integracji z rozwiązaniami klasy SIEM.

5.4. W zakresie integracji z systemami SIEM Moduł AntySpam musi:

5.4.1. wspierać przynajmniej następujące formaty:

5.4.1.1. CEF – Common Event Format,

5.4.1.2. LEEF - Log Event Extended Format,

5.4.1.3. Para klucz – wartość,

5.4.1.4. Własny, w oparciu o wbudowane szablony,

5.4.2. wspierać zarówno protokół TCP oraz UDP.

5.4.3. umożliwiać dostosowywanie i formatowanie logów osobno dla poszczególnych faz przetwarzania wiadomości, minimum:

5.4.3.1. Informacje o połączeniu SMTP

5.4.3.2. Informacje o wiadomości i jej przetwarzaniu przez polityki

5.4.3.3. Informacje o dostarczeniu wiadomości do kolejnego serwera

5.4.3.4. Akcje administracyjne (audit log)

5.5. Moduł AntySpam musi umożliwiać integrację z rozwiązaniami do szyfrowania wiadomości (tzw. Email Encryption Gateway) firm trzecich.

5.6. Moduł musi umożliwiać integrację z rozwiązaniem bezpieczeństwa web tego samego producenta i być przystosowany do takiej rozbudowy.

5.7. Moduł musi zapewniać funkcję ochrony wrażliwych danych (DLP) w komunikacji email, umożliwiając identyfikację chronionych informacji z użyciem mechanizmów:

5.7.1. słowa kluczowe,

5.7.2. słowniki,

5.7.3. wyrażenia regularne,

5.7.4. właściwości przesyłanych plików takie jak prawdziwy typ pliku, jego nazwa lub rozmiar,

5.7.5. cyfrowe identyfikatory (fingerprint) tworzone dla danych nieuporządkowanych takich jak pliki na serwerach plików,

5.7.6. cyfrowe identyfikatory (fingerprint) tworzone dla danych uporządkowanych np. przechowywanych w bazach danych,

5.7.7. mechanizm uczenia maszynowego potrafiący rozpoznać cechy charakterystyczne dla dokumentów danego rodzaju tworzonych w organizacji

na podstawie nauki przeprowadzonej w oparciu o zestawy dokumentów treningowych.

5.8. Moduł musi umożliwiać wykrywanie treści chronionych mechanizmami wymienionymi w poprzednim punkcie również w przesyłanych plikach graficznych wykorzystując technologię OCR (ang. Optical Character Recognition).

5.9. Moduł musi zawierać wbudowane zestawy reguł i polityk ochrony danych oraz kreator ułatwiający ich wybór, które znacznie przyspieszają proces wdrożenia rozwiązania dostarczając ochrony dla popularnych typów danych, np. w celu uzyskania zgodności z różnymi regulacjami.

5.10. Moduł musi zawierać predefiniowane reguły ochrony oraz mechanizmy identyfikacji danych takich jak numery kart kredytowych, IBAN, oraz identyfikatorów jak PESEL, REGON, NIP, czy numer dowodu osobistego, łącznie z weryfikacją poprawności tych identyfikatorów poprzez sprawdzenie sumy kontrolnej.

5.11. Moduł musi udostępniać wbudowany mechanizm zabezpieczania poufnych wiadomości w ten sposób, że adresat otrzymuje powiadomienie o czekającej na niego wiadomości, z którą może się zapoznać po zalogowaniu się do specjalnego portalu udostępnianego bezpośrednio na bramce email w ramach systemu.

5.12. Moduł musi umożliwiać współdzielenie zdefiniowanych tych samych polityk DLP z modułem ochrony dostępu do sieci Internet (Proxy), bez konieczności ich ręcznego przepisywania między modułami.

6. Wymagania funkcjonalne i techniczne dla Modułu AntyMalware

6.1. 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.

6.2. Architektura Modułu AntyMalware musi składać się z:

6.2.1. Centralnego serwera zarządzania Modułu AntyMalware, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa dodatkowej ochrony poczty elektronicznej i raportowania oraz

6.2.2. 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).

6.3. 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.

6.4. Analizatory dynamiczne Modułu AntyMalware muszą działać w postaci klastra nadmiarowego. Klaster odporny na awarie musi być dostarczony jednej lokalizacji (fizyczna lokalizacja; dwa urządzenia w lokalizacji dla całego Modułu). sumarycznie minimum 2 analizatory.

6.5. Integracja z posiadanym serwerem centralnego zarządzania musi umożliwiać przynajmniej zarządzanie alertami pochodzącymi z analizatorów dynamicznych, możliwość zwalniania z kwarantanny zatrzymanych wiadomości, zarządzanie politykami bezpieczeństwa na wszystkich klastrach analizatorów jednocześnie i możliwość wykonywania bezpośredniej aktualizacji oprogramowania analizatorów.

6.6. Moduł AntyMalware musi integrować się z system SIEM i zasilać go wszelkimi wykrytymi zdarzeniami bezpieczeństwa

6.7. 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)

6.8. 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.

6.9. 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.

6.10. 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.

6.11. Analizator dynamiczny musi umożliwiać wdrożenie w następujących trybach:

6.11.1. in-line - urządzenie działa jako MTA będąc pośrednikiem w ruchu email do serwerów poczty,

6.11.2. monitorowania - przez podłączenie do portu SPAN przełącznika sieciowego lub do urządzenia typu TAP,

6.11.3. BCC – do urządzenia dociera kopia oryginalnych maili poprzez protokół SMTP (generowanych przez bramkę pocztową lub serwer pocztowy).

6.12. Analizator dynamiczny musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa redundantne dyski pracujące w RAID.

6.13. 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:

6.13.1. po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie złośliwego email w kwarantannie,

6.13.2. 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,

6.13.3. 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.

6.14. 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.

6.15. Cała analiza załączników w celu wykrycia ataków w poczcie email musi odbywać się w infrastrukturze Odbiorcy.

6.16. 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, w celu utrudnienia wykrycia rodzaju środowiska wirtualnego przez podlegające analizie dynamicznej próbki złośliwego oprogramownia .

6.17. Moduł AntyMalware musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty email niezależnie od użytego rozszerzenia pliku.

6.18. Moduł AntyMalware musi analizować i blokować niebezpieczne treści dla załączników takich jak:

6.18.1. plików wykonywalnych (EXE,MSI),

6.18.2. dokumentów (PDF, RTF),

6.18.3. plików Java (JAR, JS, JSE),

6.18.4. plików z pakietu MS Office,

6.18.5. plików multimedialnych (FLASH),

6.18.6. plików skompresowanych (RAR, ZIP, 7ZIP, GZIP, SFX),

6.18.7. skrótów MS Windows (LNK),

6.18.8. plików www (HTML, HTM),

6.18.9. plików z bibliotekami (DLL),

6.18.10. plików zawierających skrypty (Powershell, VBS, BAT, CMD, VBE, VB, COM),

6.19. Moduł AntyMalware musi zostać wdrożony w trybie "in-line" w trybie aktywnego blokowania zainfekowanych wiadomości email i umieszczać je w lokalnej kwarantannie

6.20. 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.

6.21. Moduł AntyMalware musi automatycznie tworzyć reguły umożliwiające blokowanie zagrożeń na podstawie:

6.21.1. wyników analizy malware wykonanej na danym urządzeniu,

6.21.2. danych przekazanych z centralnego systemu zarządzania, pochodzących z wyników analizy wykonanych na innych urządzeniach Modułu AntyMalware w środowisku Odbiorcy,

6.21.3. danych dostępnych z centralnego repozytorium producenta (centrum reputacyjne Producenta).

6.22. Moduł AntyMalware musi umożliwiać stosowanie własnych reguł opisujących parametry z nagłówków wiadomości email (header) i na tej podstawie wykrywać groźne wiadomości pocztowe.

6.23. Moduł AntyMalware musi posiadać dodatkowe, uzupełniające mechanizmy chroniące pocztę email Odbiorcy przed atakami:

6.23.1. phishing / spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających),

6.23.2. impersonation (CEO fraud) - kompromitacja kadry zarządzającej w celu kradzieży informacji,

6.23.3. infekcją kodu JavaScript, VBScript,

6.23.4. spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.

6.23.5. 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);

6.24. 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.

6.25. 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.

6.26. 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.

6.27. 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:

6.27.1. adres nadawcy i adres odbiorcy,

6.27.2. analiza nagłówka wiadomości (header)

6.27.3. body wiadomości,

6.27.4. wyniki analizy załączników i adresów URL,

6.27.5. informacje kontekstowe na temat wykrywanego zagrożenia malware, adware, spyware,

6.27.6. funkcja skrótu (HASH), przynajmniej MD5 i SHA256

6.28. 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).

6.29. 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.

6.30. Moduł AntyMalware musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnej wiadomości email).

6.31. Moduł AntyMalware musi posiadać dodatkowy mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:

6.31.1. skrypty przesyłane w wiadomości email,

6.31.2. pliki wykonywalne przesyłane w załączniku lub URL,

6.31.3. dokumenty MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym,

6.31.4. nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO,

6.31.5. wiadomości email ze skróconymi linkami (tiny URL),

6.31.6. dokumenty MS OFFICE z flash,

6.31.7. pliki JAR,

6.31.8. hasła z formularzy przesyłanych w formie HTTP request,

6.31.9. zaszyfrowane pliki PDF,

6.31.10. pliki typu wygaszacz ekranu,

6.31.11. nieznanych plików konfiguracyjnych .SettingContent-ms.

6.31.12. zaszyfrowane dokumenty MS Office

6.31.13. Dokumenty MS Office z obiektami Embedded Object

6.31.14. Dokumenty PDF, HWP lub MS Office z aktywnością sieciową

6.31.15. pliki MS Office z makrem tworzącym plik wykonywalny

6.31.16. uszkodzone pliki wykonywalne PE

6.31.17. obiekty próbujące wykryć rozwiązania AV/Firewall za pomocą WMI

6.31.18. pliki z niezgodnym rozszerzeniem (innym niż w magic byte)

6.31.19. dokumenty Office z zagnieżdżonymi obiektami SWF

6.32. 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).

6.33. 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”).

6.34. 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.

6.35. 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.

6.36. Moduł AntyMalware musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Odbiorcę, opisujących cechy podejrzanych obiektów w formacie Yara.

6.37. Moduł AntyMalware musi umożliwiać generowanie raportów zawierających co najmniej:

6.37.1. statystyki wykrytych alertów, typy i opis wykrytych zagrożeń, akcje podjęte w związku z wykrytym zagrożeniem,

6.37.2. statystyki przeanalizowanych wiadomości email,

6.37.3. statystyki analizowanej poczty, z podziałem na poszczególne godziny, w celu oceny obciążenia systemu

6.38. 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).

6.39. Moduł AntyMalware musi generować automatycznie (za pomocą wbudowanej funkcji) raport z analizy dynamicznej, zarówno dla graficznej reprezentacji wyniku analizy jaki i wykonanych po sobie czynności krok po kroku.

6.40. 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).

6.41. 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

6.42. 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.

6.43. 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.

3. Moduł ochrony dostępu do sieci Internet:

7) Moduł musi umożliwiać monitorowanie i kontrolę połączeń do sieci www z wykorzystaniem protokołów HTTP i HTTPS.

8) Moduł musi filtrować ruch http/https porównując odwołania ze specjalizowaną bazą danych (dostarczaną przez producenta) podzieloną na kategorie (np. Sport, Adult Material, Entertainment, Shopping, Travel, etc). Rozwiązanie musi posiadać co najmniej 80 kategorii dla ruchu web.

9) Moduł musi umożliwiać tworzenie własnych kategorii i dodawanie do nich zarówno tych URL, których nie ma w bazie dostarczanej przez producenta jak i tych, które się tam znajdują, ale w innej kategorii.

   i. Wspomniane nadanie lub zmiana kategorii musi być możliwa poprzez definicję adresu URL, słowa kluczowego lub wyrażenia regularnego.

10) Moduł Proxy musi udostępniać interfejs REST API umożliwiający zautomatyzowane zarządzanie własnymi kategoriami stron i zasilanie ich informacjami o adresach URL oraz IP bez konieczności korzystania z konsoli zarządzającej.

11) Baza adresów URL musi być nieprzerwanie aktualizowana przez producenta min. poprzez stosowanie:

   i. specjalnych robotów internetowych przeszukujących i analizujących zasoby sieci,
   ii. mechanizmów sztucznej inteligencji dokonujących klasyfikacji zawartości stron,
   iii. zespoły wsparcia technicznego producenta, weryfikujących poprawność klasyfikacji.

12) Baza producenta musi mieć możliwość automatycznego pobierania aktualizacji od producenta. Ponadto dla stron, na które wchodzili pracownicy firmy, a które nie były skategoryzowane w bazie, musi istnieć możliwość ich automatycznego wysyłania do producenta w celu kategoryzacji.

13) Moduł Proxy musi także analizować pozostały ruch sieciowy i rozpoznawać jego rodzaj. Administrator systemu musi mieć możliwość zabronić lub zezwolić na wykorzystanie przez użytkowników określonych protokołów – np. powinna istnieć możliwość zablokowania protokołów IRC, P2P, IM. Protokoły sieciowe powinny być podzielone na kategorie (np. Instant

Messaging, P2P File Transfer, etc). Moduł musi posiadać co najmniej 80 protokołów podzielonych na co najmniej 10 kategorii.

14) Analiza i rozpoznawanie musi dotyczyć również protokołów tunelowanych w połączeniach HTTP i HTTPS.
15) Moduł musi umożliwiać tworzenie własnych definicji protokołów.
16) Moduł Proxy musi umożliwiać zarządzanie ruchem użytkowników w oparciu o:
    i. Kategorie stron internetowych
    ii. Protokół sieciowy
    iii. Aplikacje w chmurze
17) W przypadku zarządzania w oparciu o aplikacje w chmurze do ich identyfikacji musi być wykorzystywana specjalizowana baza utrzymywana i rozwijana przez Producenta zawierająca aplikacje dostępne dla użytkowników.
18) W zakresie zarządzania aplikacjami w chmurze administrator może określić wprost aplikacje, które mają być dostępne lub blokowane dla użytkowników jak również wskazać, iż blokowane powinny być wszystkie aplikacje dla których producent określił poziom związanego z ich wykorzystaniem przez pracowników ryzyka jako wysoki.
19) Moduł Proxy musi posiadać zintegrowaną funkcjonalność buforowania ruchu (cache proxy).
20) Moduł Proxy musi umożliwiać wdrożenie w dwóch trybach:
    i. jawne proxy (explicit proxy), gdy przeglądarki na komputerach w sieci muszą zostać skonfigurowane ręcznie lub z wykorzystaniem mechanizmów PAC (Proxy Auto Configuration) oraz WPAD (Web Proxy Auto Discovery),
    ii. przezroczyste proxy (transparent proxy), gdy ruch z komputerów jest przekierowywany na serwer proxy w sieci. W tym drugim przypadku przekierowanie ruchu na serwer proxy musi być możliwe z wykorzystaniem przełącznika sieciowego i informacji dostępnych w warstwie 4 modelu ISO/OSI, trasowania opartego o polityki (PBR - policy based routing) lub protokołu WCCP v2, w szczególności z CISCO ASA.
21) Moduł Proxy musi w ramach WCCP umożliwiać:
    i. Zastosowanie więcej niż jednego serwera proxy wraz z ich klastrowaniem,
    ii. Kierowanie ruchu na wybrany serwer proxy w klastrze na podstawie mechanizmu hash'owania wybranej kombinacji lub maskowania jednego z następujących atrybutów ruchu:
        1. Źródłowy adres IP
        2. Źródłowy port
        3. Docelowy adres IP
        4. Docelowy port

iii. Przekierowywanie pakietów metodą:
    1. L2
    2. GRE
iv. Zachowanie adresu klienta podczas komunikacji z serwerem docelowym, często określane jako IP Spoofing.
v. Tworzenie tzw “reverse service group” dla właściwego kierowania ruchu powrotnego na serwer proxy potrzebnego przy włączonej funkcji IP Spoofing.

22) Musi istnieć możliwość równoczesnego korzystania z serwera proxy przez klientów w trybie jawnym (np. mechanizm WPAD) i przezroczystym (np. WCCP) z możliwością niezależnego konfigurowania funkcji zachowania adresu klienta dla tych trybów pracy serwera proxy. Dodatkowo musi być możliwe określanie różnych adresów IP za którymi będą „ukrywani” przez serwer proxy klienci łączący się z określonych adresów IP lub zakresu adresów IP.
23) Modul Proxy musi oferować funkcje DNS Proxy, FTP Proxy, oraz protokół SOCKS.
24) Wymagane jest, aby dostarczony Moduł Proxy mógł zostać skonfigurowany dla poprawnego działania we współpracy z innymi serwerami proxy (np. Microsoft ISA/TMG) w konfiguracji hierarchicznych łańcuchów proxy (proxy chaining), zarówno jako serwer podrzędny (downstream) oraz nadrzędny (upstream).
25) W przypadku, gdy dostarczone Moduł Proxy zostanie wdrożony jako nadrzędny musi potrafić skorzystać z informacji dotyczących uwierzytelnionego użytkownika, jeżeli tylko są one dostarczane przez podrzędne proxy w nagłówkach X-Forwarded-For oraz X-Authenticated-User.
26) Modul Proxy musi umożliwiać uwierzytelnienie użytkowników z wykorzystaniem następujących mechanizmów:
    i. Zintegrowanego, wykorzystującego Kerberos jako metodę podstawową i NTLMv2 jako metodę zapasową
    ii. NTLM
    iii. LDAP
    iv. Captive Portal
27) Moduł Proxy musi umożliwiać uwierzytelnianie użytkowników również w przypadku wdrożenia w trybie transparent proxy.
28) Moduł Proxy musi umożliwiać tworzenie reguł uwierzytelniania pozwalających kontrolować ruch z których sieci i z użyciem których aplikacji (user agent) należy uwierzytelniać w jaki sposób oraz wobec której domeny.
29) Moduł Proxy musi umożliwiać uwierzytelnianie użytkowników za pomocą certyfikatów.

30) Moduł Proxy musi umożliwiać kategoryzację odwiedzanych przez użytkowników stron internetowych na podstawie ich bieżącej zawartości. Musi być możliwe ograniczenie analizy zawartości stron internetowych w czasie rzeczywistych do tych, których nie ma w bazie URL dostarczanej przez producenta oraz kilku kategorii wskazanych przez producenta. Ta funkcjonalność musi w szczególności dotyczyć dynamicznych stron Web 2.0.
31) Moduł Proxy musi umożliwiać zarządzanie możliwością wykonywania w ramach popularnych portali społecznościowych wybranych funkcji takich jak np. użycie funkcji chat, publikowanie komentarzy, zdjęć, materiałów video.
32) Moduł Proxy musi umożliwiać usuwanie aktywnej zawartości jak ActiveX, JavaScript, oraz VBScript z zawartości serwowanej użytkownikom.
33) Moduł Proxy musi umożliwiać blokowanie złośliwej zawartości jak szkodliwe oprogramowanie i wirusy z wykorzystaniem zarówno tradycyjnego skanowania antywirusowego jak i zaawansowanych technik wykrywania zagrożeń jak heurystyka.
34) Moduł Proxy musi umożliwiać administratorom zarządzanie dostępem do stron o określonej ocenie reputacji przedstawiając następujące kategorie stron internetowych:
    i. strony które mogą maskować swoją tożsamość używając usług dynamicznego DNS,
    ii. strony, które obecnie niekoniecznie serwują niebezpieczną zawartość, ale są z tego znane,
    iii. strony, których nazwa została zarejestrowana niedawno,
    iv. strony z podejrzaną zawartością
35) Polityki dotyczące skanowania bezpieczeństwa zawartości muszą umożliwiać tworzenie wyjątków dla poszczególnych stron internetowych w zakresie kategoryzacji zawartości, skanowania zagrożeń bezpieczeństwa oraz usuwania aktywnej zawartości.
36) Moduł Proxy musi blokować dostęp do stron związanych z takimi zagrożeniami jak spyware, phishing, keylogging, oraz złośliwy kod mobilny. Rozwiązanie musi także blokować ruch wychodzący do internetu generowany przez oprogramowanie typu spyware obecne na zainfekowanych komputerach w sieci.
37) Moduł Proxy musi wykrywać wysyłanie plików zawierających hasła oraz plików archiwizowanych z wykorzystaniem niestandardowych mechanizmów w celu wykrywania komunikacji skompromitowanych maszyn z serwerami na zewnątrz organizacji.
38) Administrator systemu musi mieć możliwość zabronić lub zezwolić na dostęp pracowników firmy do stron z określonych kategorii korzystając z takich wyznaczników jak użytkownik, grupa użytkowników, adres IP stacji, zakres adresów IP, dzień tygodnia, pora dnia, lub czas przebywania w danych ośrodkach web.

39) Moduł Proxy musi umożliwić użytkownikowi uzyskanie dostępu do strony z zablokowanej kategorii na podstawie znajomości hasła. Musi istnieć możliwość definiowania indywidualnych haseł użytkowników jak również dla ich grup.
40) Moduł Proxy musi oprócz blokowania dostępu do stron wybranych kategorii umożliwiać wyświetlenie na ekranie użytkownika informacji, iż strona, którą chce wyświetlić jest zabroniona przez politykę firmy z możliwością wejścia na tą stronę po świadomym wyrażeniu chęci przez użytkownika.
41) Moduł Proxy musi umożliwiać pełne dostosowanie stron z komunikatami dla użytkowników do własnych potrzeb, wliczając zmiany komunikatów oraz grafiki, np. umieszczenie własnego logo.
42) Administrator systemu musi mieć możliwość tworzenia polityki dostępu do zasobów Internetu także w oparciu o zajętość pasma sieciowego. Np. musi istnieć możliwość zabronienia dostępu do określonych kategorii, gdy zajętość pasma sieciowego wyniesie 50%, itp.
43) Dodatkowo tworzenie polityki dostępu do stron internetowych musi uwzględniać również:
    i. Słowa kluczowe zawarte w adresie URL
    ii. Typy plików
44) Moduł Proxy musi posiadać możliwość przezroczystej identyfikacji użytkowników wychodzących do Internetu oraz pozwalać na integrację z następującymi usługami katalogowymi Active Directory umożliwiając egzekwowanie polityk przypisanych do indywidualnych użytkowników lub ich grup.
45) W przypadku braku informacji identyfikujących użytkownika musi istnieć możliwość wymuszenia uwierzytelnienia użytkownika przez Rozwiązanie lub egzekwowanie polityki przypisanej dla adresu IP/zakresu adresów IP.
46) Moduł Proxy musi być wyposażone w moduł logowania aktywności użytkowników do bazy danych, z której czerpane będą dane przez moduł raportujący na potrzeby prezentacji raportów.
47) Moduł Proxy musi umożliwiać integrację z systemem SIEM (Security Information and Event Management) poprzez syslog. moduł musi umożliwiać integrację z różnymi systemami klasy SIEM, co najmniej ze Splunk
48) Moduł Proxy musi być wyposażony w element raportujący, umożliwiający:
    i. Generowanie raportów z podziałem na pojedynczych użytkowników ich grupy, kategorie i protokoły. Raporty te muszą być dostępne przez przeglądarkę.
    ii. Generowanie w/w raportów ale z ukryciem danych pozwalających zidentyfikować użytkownika (na raporcie zamiast adresu IP, nazwy, loginu itp., musi być identyfikatory nieznaczące – np. liczby).

iii. Bieżący wgląd w aktywność użytkowników.
iv. Przedstawianie informacji na temat wykorzystywanych przez użytkowników aplikacji w chmurze wraz z poziomem ryzyka związanym z wykorzystaniem poszczególnych aplikacji.
v. Prezentowanie informacji o wykorzystywanych przez użytkowników systemach operacyjnych oraz przeglądarkach, z dokładnością do nagłówka user-agent.

49) Przeglądanie aktywności użytkowników musi wykorzystywać takie kryteria jak:
i. Adres URL
ii. Kategoria adresu URL
iii. Źródłowy adres IP
iv. Docelowy adres IP
v. Port
vi. Protokół
vii. Grupa protokołów
viii. Domena
ix. Grupa użytkowników
x. Użytkownik
xi. Akcja
xii. Dzień

50) Aktywność użytkowników musi być przedstawiana z wykorzystaniem miar takich jak:
i. Ilość żądań (Hit) lub wizyt (wyświetleń stron)
ii. Ilość danych wysłanych w KB
iii. Ilość danych pobranych w KB
iv. Ilość danych (wysłanych + pobranych) w KB
v. Czas przeglądania

51) Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie musi być dostępne przez zintegrowaną webową konsolę administracyjną z możliwością delegacji uprawnień do administrowania poszczególnymi składnikami i opcjami systemu.

52) Moduł Proxy musi umożliwiać delegowanie uprawnień do zarządzania i raportowania zarówno dla użytkowników domenowych jak i użytkowników tworzonych w bazie oprogramowania filtrującego.

53) Delegowanie uprawnień musi opierać się o role administracyjne i umożliwiać przypisanie określonych uprawnień wskazanym administratorom w stosunku do wskazanych użytkowników.

54) W przypadku delegacji uprawnień musi być możliwe zablokowanie przez administratora nadrzędnego możliwości odblokowania wybranych kategorii przez administratora podrzędnego.
55) Aadministrator oprogramowania filtrującego musi mieć możliwość wglądu w szczegółowy audyt aktywności pozostałych administratorów zawierający następujące informacje:
    i. Data akcji,
    ii. Nazwa administratora, który przeprowadził akcję
    iii. Element, na którym podejmowana jest akcja,
    iv. Akacja (np. zalogowanie, wylogowanie, oraz dodanie, zmiana i usunięcie obiektu),
    v. W przypadku zmiany obiektu jego poprzednia i obecna wartość.
56) Dostęp do webowej konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https.
57) Konsola zarządzająca musi zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystki jak najpopularniejsze kategorie, najczęściej blokowani użytkownicy, oraz inne. Musi istnieć możliwość dostosowania tego widoku do własnych potrzeb. Ekran ten musi również zawierać ostrzeżenia dotyczące poprawności pracy poszczególnych komponentów oprogramowania.
58) Moduł Proxy musi umożliwiać inspekcję i zarządzanie szyfrowanymi połączeniami HTTPS.
59) Podczas nawiązywania połączenia z komputera użytkownika do serwera docelowego serwer proxy musi móc przeprowadzić kontrolę najważniejszych aspektów związanych z certyfikatem jakim legitymuje się serwer docelowy, włączając w to:
    i. zgodność adresu zawartego w certyfikacie (podmiot certyfikatu) i żądanego przez użytkownika,
    ii. datę ważności certyfikatu,
    iii. kontrolę pełnego łańcucha certyfikacji,
    iv. unieważnienie certyfikatu z wykorzystaniem CRL oraz OCSP.
60) Moduł Proxy musi utrzymywać i umożliwiać administratorom zarządzanie listą zaufanych głównych urzędów certyfikacji (Trusted Root CA) wykorzystywaną przy weryfikowaniu certyfikatów serwerów docelowych. Lista ta musi też ulegać automatycznej aktualizacji.
61) Możliwa musi być konfiguracja, w której użytkownicy są ostrzegani przed nieprawidłowościami związanymi z certyfikatem serwera docelowego, ale mogą kontynuować przeglądanie. Informacje o takich zdarzeniach muszą być widoczne w konsoli zarządzającej w postaci incydentów umożliwiających zdefiniowanie administratorowi akcji dla takich połączeń w przyszłości. Akcje muszą zawierać co najmniej:
    i. blokowanie, ale z możliwością kontynuowania, jeżeli taka opcja jest globalnie włączona dla użytkowników,

ii. blokowanie bez możliwości kontynuowania dla tej strony, nawet jeżeli taka opcja jest globalnie włączona dla użytkowników,
iii. wyłączenie inspekcji https dla tej strony, czyli tunelowanie połączenia przez proxy.

62) Musi być możliwe dostosowanie stron wyświetlanych użytkownikom w przypadku wykrytych przez proxy nieprawidłowości oraz błędów.
63) Moduł Proxy musi umożliwiać wyłączenie skanowania połączeń HTTPS dla określonych adresów URL oraz kategorii stron internetowych zapewniając zachowanie prywatności przez użytkowników korzystających np. z serwisów bankowości internetowej.
64) Moduł Proxy musi umożliwiać zarządzanie połączeniami do serwerów docelowych wymagających certyfikatu klienta w celu uwierzytelnienia połączenia.
65) Moduł Proxy musi umożliwiać zaimportowanie certyfikatu wraz z kluczem prywatnym, który zgodnie z konfiguracją administratora będzie wykorzystywany przy nawiązywaniu połączeń do określonych stron w przypadku, gdy serwer docelowy zażąda uwierzytelnienia klienta certyfikatem.
66) Konsola zarządzająca dla Modułu Proxy musi udostępniać dostęp do aktualnych oraz historycznych danych dotyczących działania serwera proxy jak:
    i. Ilość operacji na sekundę
    ii. Przepustowość w Mbit na sekundę
    iii. Współczynnik trafień dla serwera cache
    iv. Wykorzystanie przestrzeni cache na dysku
    v. Wykorzystanie przestrzeni cache w pamięci RAM
    vi. Wykorzystanie cache DNS
    vii. Błędy http
    viii. Obciążenie procesora
67) Architektura Modułu Proxy musi składać się z centralnego serwera zarządzania, służącego do zarządzania politykami bezpieczeństwa, raportowania i serwerów proxy.
68) Centralny serwer zarządzania i raportowania Moduł Proxy może być dostarczany w postaci oprogramowania (maszyna wirtualna).
69) Centralny serwer zarządzania musi umożliwiać logowanie do systemu z wykorzystaniem kont lub grup użytkowników z usługi katalogowej, np. Microsoft Active Directory.
70) Centralny serwer zarządzania musi umożliwiać konfigurację uprawnień dla administratorów systemu na podstawie skonfigurowanych ról. Role muszą pozwalać przynajmniej na konfigurację następujących poziomów dostępu:
    i. Brak dostępu do wybranej funkcji systemu.
    ii. Dostęp tylko do odczytu.

iii. Pełny dostęp.

71) Centralny serwer zarządzania Modułu Proxy musi posiadać wspólną konsolę do zarządzania modułem AntySpam (ochrona poczty).

72) Moduł Proxy musi składać się z przynajmniej czterech serwerów proxy (po dwa w każdej lokalizacji), które muszą być dostarczone w postaci:

i. rozwiązania sprzętowego na dedykowanej platformie dostarczanej przez tego samego producenta w formie urządzenia do montażu w szafie rack o następujących minimalnych wymaganiach sprzętowych:

1. Dwa procesory Intel Xeon Silver seria 4000
2. Pamięć RAM 32 GB
3. Dwa zasilacze 700W, wymienne w trakcie pracy (Hot Swappable)
4. Cztery interfejsy sieciowe RJ-45 w standardzie Ethernet 1GbE oraz dwa porty SFP z możliwością zamontowania wkładek 10Gbe i 1Gbe
5. Trzy dyski twarde o pojemności 300GB z obsługą RAID-5 wymienne w trakcie pracy (Hot Swappable)
6. Wysokość urządzenia 1U w szafie Rack
7. Moduł zdalnego awaryjnego zarządzania serwerem z dostępem do wirtualnej konsoli serwera

73) Serwer proxy musi umożliwiać konfigurację adresów IP na różnych interfejsach sieciowych. Minimalna liczba adresowalnych interfejsów sieciowych nie może być mniejsza niż trzy. System musi pozwalać na adresację interfejsów sieciowych z zachowaniem segmentacji, nie jest dopuszczalna segmentacja wykorzystująca wirtulane sieci VLAN.

74) Moduł Proxy musi posiadać funkcjonalność zarządzania serwerami proxy, zarówno serwerami sprzętowymi jak i maszynami wirtualnymi, uruchomiony na centralnym serwerze zarządzania. Moduł Proxy musi być zintegrowany z centralnym serwerem zarządzania, musi być obsługiwany przez przeglądarkę internetową oraz musi posiadać minimum następujące funkcje:

i. Dostęp do stanu usług oraz stanu obciążenia wybranej bramy.
ii. Konfigurację adresów IP dla poszczególnych interfejsów bramy.
iii. Konfigurację adresów DNS wykorzystywanych przez poszczególne moduły bramy.
iv. Konfigurację tras routingu.
v. Konfigurację kopii zapasowych.
vi. Konfigurację powiadomień SNMP.

vii. Pobieranie i instalowanie poprawek oraz nowych wersji systemu dla skonfigurowanych grup urządzeń w sposób automatyczny. Nie jest dopuszczalne wykonywanie aktualizacji jedynie w sposób ręczny, pobierając i instalując pojedyncze poprawki.

4. Moduł do analizy złośliwych plików:
   1) Zamawiający wymaga, aby sandbox (serwer) jako element Systemu posiadał wydajność umożliwiającą wykonanie co najmniej 9000 analiz dziennie.
   2) Zamawiający wymaga, aby analiza próbek była realizowana w izolowanym środowisku funkcjonującym na dedykowanym, fizycznym urządzeniu typu appliance (APP).
   3) Zamawiający wymaga, aby analiza próbek była realizowana w całości w infrastrukturze Odbiorcy, gdzie cały proces analizy musi się odbywać w tym środowisku wirtualnym. Nie jest dopuszczalne wysyłanie analizowanych plików/obiektów poza to środowisko (dopuszczalne jest jedynie wysyłanie cech charakterystycznych np. sum kontrolnych plików).
   4) Zamawiający wymaga, aby sandbox służący do analizy próbek malware był wyposażony w maszyny wirtualne wykonujące równolegle analizę dynamiczną próbek malware (w tym także adresów URL) w różnych wersjach systemu operacyjnego i aplikacji jednocześnie (co najmniej: posiadane przez Odbiorcę systemy Windows XP, Windows 7 SP1, Windows 10, MacOS) oraz różnych aplikacji i ich różnych wersji zainstalowanych w tych systemach (co najmniej posiadane przez Odbiorcę FireFox, Chrome, Adobe Reader, Java, MS Office). Wszystkie niezbędne licencje na systemy operacyjne i aplikacje muszą być dostarczone wraz z oferowanym Systemem.
   5) Zamawiający wymaga, aby na potrzeby analizy próbek malware (tj. uruchamiania plików w izolowanym środowisku) element Sandbox zapewniał co najmniej:
      i. by środowisko, w jakim jest wykonywana analiza dynamiczna, posiadało mechanizmy utrudniające jego wykrycie przez analizowany malware,
      ii. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku posiadały mechanizmy symulacji pracy realnego użytkownika,
      iii. możliwość nawiązania połączenia sieciowego badanej próbki umożliwiającego pobranie dodatkowej zawartości z Internetu; kontaktu z serwerami C&C, itp. (celem śledzenia działania badanej próbki w sieci),
      iv. możliwość parametryzacji środowisk wirtualnych w zakresie: nazwy domeny, folderów użytkowników, ostatnio otwartych plików, języka systemu operacyjnego, wpisania hasła w celu automatycznego odszyfrowania przekazywanej do analizy próbki malware,

v. możliwość ręcznego wysyłania próbek (plików/obiektów) jak również adresu URL do analizy dynamicznej z poziomu konsoli zarządzającej Systemu i poprzez REST API oraz możliwość prezentacji wyników tej analizy.

6) Zamawiający wymaga, aby element Systemu służący do analizy próbek malware umożliwiał generowanie raportów zawierających co najmniej wyniki analiz i statystyki przeanalizowanych próbek. Raporty powinny mieć możliwość eksportu na przykład do formatu CSV lub XML wraz z możliwością ustalenia okresu dla generowanego raportu (przykładowo: ostatnie 24 godziny, ostatnie 7 dni, ostatnie 30 dni).
7) Sandbox musi umożliwiać integrację z konsolą do zarządzania Systemem w zakresie przesyłania wskaźników kompromitacji IoC, raportowania zdarzeń, konfiguracji ustawień systemu, aktualizacji oraz weryfikacji aktualnego stanu urządzenia.

5. Moduł do ochrony udziałów sieciowych:
   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, htm, ico, jar, , jpg, mov, mp4, pdf, png, 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:
    i. środowisko, w jakim jest wykonywana analiza dynamiczna, musi posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware,

ii. 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 muszą 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 Odbiorcę 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.

6. Moduł do zarządzania:
    1) System musi pozwalać na zarządzanie innymi komponentami zaproponowanego rozwiązania oraz wszystkimi ich parametrami (np.: konfiguracja trybów pracy, konfigurację zasad alarmowania, zasad eksportu danych do innych systemów bezpieczeństwa, zasad wykonywania kopii bezpieczeństwa, propagowanie poprawek i aktualizacje oprogramowania, zarzadzanie licencjami).
    2) Korzystanie z centralnego systemu zarządzania musi odbywać się przy pomocy interfejsu graficznego dostępnego zdalnie, przy wykorzystaniu przeglądarki internetowej oraz poprzez wiersz poleceń przy wykorzystaniu klienta SSH.
    3) Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu, jak również komunikacja sieciowa pomiędzy poszczególnymi jego elementami, musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.
    4) Zarządzanie Systemem powinno być dostępne jako platforma on-prem.
    5) System zarządzania powinien zapewniać co najmniej:
    6) automatyczną korelację wyników analiz między modułami, zwłaszcza pochodzących z analizy próbek malware,
    7) przegląd wyników analiz z wszystkich elementów Systemu,
    8) dostęp do statystyk z działania Systemu,
    9) możliwość tworzenia kont użytkowników Systemu o różnych poziomach uprawnień,
    10) logowanie i przegląd działań w Systemie.
    11) System musi udostępniać możliwość integracji z systemem klasy SIEM poprzez API (preferowany otwarty standard RESTful Interface lub co najmniej syslog).

7. Wymagania w zakresie dokumentacji:
    1) Wykonawca w uzgodnieniu z Zespołem Odbiorowym opracuje i dostarczy następującą Dokumentację Projektową:
        i. 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,
        ii. 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:
   i. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
   ii. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
   iii. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
   iv. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zespołu Odbiorowego.
3) Dokumentacja musi być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.

8. 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:
      i. zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
      ii. 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,
      iii. 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.

9. Wymagania w zakresie wdrożenia**:**
    1) Odbiorca dostarczy wszystkie niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu 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:
        i. odbiór Systemu ochrony poczty elektronicznej wraz z wchodzącymi w skład Systemu Modułami ochrony, na podstawie przeprowadzonych Testów Akceptacyjnych,
        ii. odbiór Dokumentacji Powykonawczej,
        iii. odbiór realizacji transferu wiedzy.

Maksymalny termin dostawy, wdrożenia, uruchomienia i konfiguracji Systemu – 21 dni.