

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

**Zakup systemu bezpieczeństwa poczty elektronicznej wraz z rocznym
wsparciem technicznym producenta**

Spis treści

I. Przedmiot zamówienia	3
II. Nazwy i kody Wspólnego Słownika Zamówień (CPV)	3
III. Zakres ilościowy zamówienia	4
IV. Wymagania ogólne dotyczące realizacji zamówienia.....	5
V. Wymagania funkcjonalne i techniczne (wymagania minimalne).....	7
VI. Wdrożenie	16
VII. Wsparcie techniczne i serwis.....	17
VIII. Równowaga (klauzula równowagi)	17
IX. Gwarancja, dostępność i poziom świadczenia usług	18
X. Wymagania dotyczące producenta rozwiązania i bezpieczeństwa danych	18

I. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz utrzymanie systemu bezpieczeństwa poczty elektronicznej (Email Security) w modelu hybrydowym, chroniącego pocztę przychodzącą i wychodzącą Zamawiającego przed zagrożeniami, w tym przed phishingiem, atakami typu BEC, złośliwym oprogramowaniem, ransomware oraz przejęciem konta. Podstawowe moduły zabezpieczające (warstwa bramy pocztowej) muszą zostać wdrożone w modelu lokalnym (on-premise), natomiast zaawansowane funkcjonalności analizy zagrożeń — analiza załączników w środowisku sandbox oraz analiza i ochrona adresów URL — realizowane są jako usługi chmurowe, z zachowaniem wymagań dotyczących lokalizacji przetwarzania danych określonych w Sekcji IV. Zamówienie obejmuje także wsparcie techniczne producenta przez okres 12 miesięcy oraz wykonanie usług wdrożeniowych.

Zakres zamówienia obejmuje w szczególności:

- dostawę i wdrożenie podstawowych modułów zabezpieczających poczty w modelu lokalnym (on-premise), w infrastrukturze Zamawiającego, dla 3 600 użytkowników klasycznych oraz 900 użytkowników typu „Light” — łącznie 4 500 użytkowników, na okres 12 miesięcy;
- udostępnienie usług chmurowych w zakresie analizy załączników w środowisku sandbox (z rezydencją danych w EOG) oraz analizy i ochrony adresów URL, na okres 12 miesięcy;
- integrację z istniejącą infrastrukturą poczty i usługą katalogową Zamawiającego;
- świadczenie wsparcia technicznego producenta na podwyższonym poziomie (zgodnie z definicją w Sekcji VII) przez okres 12 miesięcy;
- przekazanie dokumentacji powykonawczej oraz instruktaż dla administratorów Zamawiającego.

II. Nazwy i kody Wspólnego Słownika Zamówień (CPV)

Przedmiot zamówienia został zaklasyfikowany pod następującymi kodami CPV:

Kod CPV	Nazwa
48730000-4	Pakiety oprogramowania zabezpieczającego
48761000-0	Pakiety oprogramowania antywirusowego
48000000-8	Pakiety oprogramowania i systemy informatyczne
72250000-2	Usługi w zakresie konserwacji i wsparcia systemów
72265000-0	Usługi konfiguracji oprogramowania
72611000-6	Usługi w zakresie technicznego wsparcia komputerowego
72000000-5	Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

III. Zakres ilościowy zamówienia

Zamawiający wymaga zapewnienia licencji oraz usług w następujących ilościach:

Lp.	Przedmiot	Liczba (szt.)	Okres	Jednostka	Uwagi
1	Podstawowe moduły zabezpieczające poczty (brama / agent MTA, antyspam, antywirus, DLP, kwarantanna, routing, DMARC) — wdrożenie lokalne (on-premise) — użytkownik klasyczny (pełna ochrona)	3 600	12 miesięcy	użytkownik	Licencja on-premise
2	Podstawowe moduły zabezpieczające poczty — wdrożenie lokalne (on-premise) — użytkownik typu „Light” (konta o ograniczonym zakresie, np. funkcyjne/współdzielone)	900	12 miesięcy	użytkownik	Licencja on-premise
3	Usługa chmurowa analizy załączników w środowisku sandbox (detonacja), z rezydencją danych w EOG	4 500	12 miesięcy	użytkownik	Usługa chmurowa
4	Usługa chmurowa analizy i ochrony adresów URL (przepisywanie linków, analiza w czasie kliknięcia)	4 500	12 miesięcy	użytkownik	Usługa chmurowa
5	Wsparcie techniczne producenta na podwyższonym poziomie (zgodnie z definicją w Sekcji VII)	1	12 miesięcy	komplet	dla 4 500 użytłk.
6	Usługi wdrożeniowe (implementacja, konfiguracja, uruchomienie)	1	jednorazowo	komplet	—

Definicja użytkowników:

Przez „użytkownika klasycznego” Zamawiający rozumie indywidualną, imienną skrzynkę pocztową przypisaną do osoby fizycznej, w szczególności pracownika, współpracownika lub innej osoby korzystającej z poczty elektronicznej Zamawiającego w sposób bieżący, obejmującą pełny zakres ochrony wymagany w OPZ.

Jeden użytkownik klasyczny liczony jest jako jedna podstawowa skrzynka pocztowa / konto pocztowe posiadające unikalny główny adres SMTP. Alias adresu, dodatkowy adres proxy, zmiana nazwy konta lub członkostwo w grupie dystrybucyjnej nie stanowią odrębnego użytkownika klasycznego.

Przez „użytkownika typu Light” Zamawiający rozumie nieimienne albo współdzielone konto pocztowe wykorzystywane w ograniczonym zakresie, w szczególności:

- skrzynkę funkcyjną, np. sekretariat@, kancelaria@, kontakt@, przetargi@, helpdesk@,
- skrzynkę współdzieloną używaną przez więcej niż jedną osobę,
- skrzynkę techniczną, aplikacyjną lub systemową,
- skrzynkę procesu biznesowego, urządzenia, usługi lub systemu,
- konto pocztowe służące głównie do odbierania powiadomień, wysyłki komunikatów systemowych albo obsługi określonej funkcji organizacyjnej.

Użytkownicy typu Light muszą być objęci co najmniej ochroną ruchu poczty przychodzącej i wychodzącej realizowaną przez warstwę bramy / agenta MTA, obejmującą antyspam, antywirus, antymalware, antyphishing, ochronę przed BEC/spoofingiem, mechanizmy DMARC/SPF/DKIM, DLP, routing, kwarantannę, logowanie, raportowanie, analizę adresów URL oraz analizę załączników w środowisku sandbox, zgodnie z wymaganiami OPZ.

Załącznik nr 1 do umowy

Jeżeli producent oferowanego rozwiązania nie posiada odrębnej kategorii licencji odpowiadającej użytkownikowi typu Light, Wykonawca zobowiązany jest uwzględnić w cenie takie licencje lub uprawnienia, które zapewnią ochronę 900 kont typu Light zgodnie z wymaganiami OPZ, bez dodatkowych kosztów dla Zamawiającego.

Wykonawca zapewni licencjonowanie obejmujące łącznie nie mniej niż 4 500 użytkowników przez cały okres obowiązywania umowy.

IV. Wymagania ogólne dotyczące realizacji zamówienia

1. Rozwiązanie musi obsługiwać pełną liczbę 4 500 licencjonowanych użytkowników bez pogorszenia parametrów wydajnościowych i bez dodatkowych, nieujętych w ofercie kosztów w okresie obowiązywania umowy.
2. Subskrypcja licencji oraz wsparcie producenta muszą obejmować nieprzerwany okres 12 miesięcy, liczony od dnia odbioru wdrożenia (lub innego dnia wskazanego w umowie).
3. Wszystkie funkcjonalności wymagane w Sekcji V muszą być dostępne w ramach oferowanej licencji, bez konieczności dokupowania dodatkowych modułów (chyba że dany moduł został wprost wskazany jako opcjonalny).
4. Konsola administracyjna oraz dokumentacja techniczna muszą być dostępne co najmniej w języku polskim lub angielskim; dokumentacja powykonawcza zostanie dostarczona w języku polskim.
5. Przetwarzanie danych (w tym treści wiadomości e-mail i danych osobowych) musi odbywać się zgodnie z RODO; Wykonawca zawrze z Zamawiającym umowę powierzenia przetwarzania danych osobowych. Przetwarzanie danych musi co do zasady odbywać się na terenie Europejskiego Obszaru Gospodarczego (EOG); jedyny dopuszczalny wyjątek dotyczy funkcjonalności sprawdzania adresów URL, na zasadach określonych w punktach poniżej.
6. Rozwiązanie musi zapewniać interoperacyjność z istniejącym środowiskiem teleinformatycznym Zamawiającego (poczta, usługa katalogowa). Wskazane w opisie nazwy systemów (np. Active Directory, Azure AD / Microsoft Entra ID, Microsoft 365, Microsoft Exchange, Microsoft Outlook, OWA, OneDrive, SharePoint, Google Workspace) służą wyłącznie opisaniu środowiska Zamawiającego oraz zapewnieniu interoperacyjności i nie stanowią preferencji wobec konkretnego producenta rozwiązania bezpieczeństwa.
7. Rozwiązanie musi być wdrożone w modelu hybrydowym. Podstawowe moduły zabezpieczające (warstwa bramy pocztowej, w szczególności agent MTA, silnik polityk bezpieczeństwa, antyspam, antywirus, DLP, kwarantanna oraz lokalny magazyn danych pocztowych) muszą być wdrożone i eksploatowane w modelu lokalnym (on-premise), w infrastrukturze Zamawiającego. Zaawansowane funkcjonalności analizy zagrożeń (analiza załączników w środowisku sandbox oraz analiza i ochrona adresów URL) mogą być realizowane jako usługi chmurowe producenta, z zachowaniem wymagań dotyczących lokalizacji przetwarzania danych określonych w punktach poniżej.
8. Podstawowe moduły zabezpieczające, stanowiące warstwę on-premise rozwiązania, muszą być możliwe do uruchomienia jako maszyny wirtualne w aktualnie eksploatowanym przez Zamawiającego środowisku wirtualizacyjnym VMware vSphere 8. Wymóg ten wynika z konieczności zapewnienia interoperacyjności z istniejącą infrastrukturą Zamawiającego i nie stanowi preferencji dla producenta platformy wirtualizacyjnej ani producenta rozwiązania bezpieczeństwa poczty. Wykonawca dostarczy obraz maszyny wirtualnej w formacie OVA/OVF albo inny pakiet instalacyjny, obraz, template lub równoważny mechanizm wdrożeniowy

Załącznik nr 1 do umowy

umożliwiający instalację i uruchomienie rozwiązania w środowisku VMware vSphere 8 bez konieczności nabywania przez Zamawiającego dodatkowej platformy wirtualizacyjnej. Za zgodność ze środowiskiem Zamawiającego uznaje się co najmniej możliwość importu, instalacji, uruchomienia, aktualizacji i wsparcia producenta dla rozwiązania działającego w środowisku VMware vSphere 8. Wykonawca dostarczy dokumentację instalacyjną i konfiguracyjną oraz wskaże wymagane zasoby maszyny wirtualnej.

9. Rozwiązanie musi umożliwiać dodawanie kolejnych wirtualnych instancji / agentów (skalowanie poziome) w celu zwiększenia wydajności, rozłożenia obciążenia oraz zapewnienia wysokiej dostępności, bez konieczności nabywania dodatkowych licencji. Licencjonowanie musi być oparte o liczbę chronionych użytkowników (4 500), niezależnie od liczby uruchomionych instancji / agentów wirtualnych oraz niezależnie od liczby obsługiwanych domen pocztowych. Również wsparcie techniczne i utrzymanie producenta nie mogą być uzależnione od liczby uruchomionych instancji / agentów wirtualnych, lecz wyłącznie od liczby chronionych użytkowników.
10. Skanowanie i analiza załączników (w tym analiza dynamiczna / detonacja w środowisku typu sandbox), niezależnie od tego, czy realizowane lokalnie czy jako usługa chmurowa, musi odbywać się wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG). Dane załączników (treść plików) nie mogą być przekazywane ani przetwarzane poza EOG.
11. Funkcjonalność sprawdzania i analizy adresów URL (linków) może wykorzystywać przetwarzanie z transferem danych do państwa trzeciego (poza EOG) wyłącznie pod warunkiem, że producent rozwiązania posiada odpowiednie instrumenty zapewniające zgodność takiego transferu z RODO (np. decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony, standardowe klauzule umowne (SCC) lub udział w programie EU–US Data Privacy Framework). Na wezwanie Zamawiającego w trakcie realizacji umowy Wykonawca wskaże podstawę prawną oraz mechanizm transferu danych realizowanego w ramach tej funkcjonalności.
12. Dostarczany obraz maszyny wirtualnej musi spełniać co najmniej minimalne wymagania zasobowe określone w tabeli poniżej, odrębnie dla węzła zarządzającego (master) oraz węzła przetwarzającego (agent).

Minimalne zasoby na pojedynczą instancję wirtualną (środowisko VMware vSphere 8), gwarantujące wymaganą wydajność:

Typ instancji wirtualnej	vCPU	RAM	Przestrzeń dyskowa
Węzeł zarządzający (master)	6	16 GB	250 GB
Węzeł przetwarzający (agent)	6	16 GB	80 GB

Powyższe wartości stanowią minimum na instancję. Liczbę węzłów przetwarzających (agentów) dobiera się stosownie do wolumenu poczty i wymagań wydajnościowych/dostępnościowych; dodawanie kolejnych instancji nie wiąże się z dodatkowymi opłatami licencyjnymi ani ze wzrostem kosztów wsparcia (zob. wymagania powyżej).

Wymagania w zakresie cyberbezpieczeństwa (zgodność z ustawą o krajowym systemie cyberbezpieczeństwa)

Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia — zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące — nie obejmowało:

Załącznik nr 1 do umowy

- a) produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
- b) produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

Niespełnienie powyższego wymagania skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 ustawy Pzp.

V. Wymagania funkcjonalne i techniczne (wymagania minimalne)

Wszystkie wymagania wymienione w niniejszej sekcji stanowią wymagania minimalne (obligatoryjne). Oferowane rozwiązanie musi spełniać każde z poniższych wymagań. Potwierdzenie spełnienia każdego wymagania Wykonawca składa w odrębnym Formularzu zgodności (matrycy spełnienia wymagań) stanowiącym załącznik do SWZ. Niespełnienie któregośkolwiek z wymagań minimalnych skutkuje uznaniem, że oferta nie spełnia wymagań Zamawiającego.

Potwierdzenie spełnienia wymagań następuje na odrębnym Formularzu zgodności składanym wraz z ofertą (załącznik do SWZ).

1. Wdrażanie i zarządzanie

Model hybrydowy: podstawowe moduły lokalnie (on-premise), zaawansowane analizy jako usługi chmurowe; integracja w przepływie poczty (inline) i przez API albo wdrożenie w oparciu o rekordy MX

Lp.	Wymaganie minimalne
1	Oferowane rozwiązanie musi być przedmiotem aktualnej, niezależnej oceny rynkowej przeprowadzonej przez renomowaną organizację analityczną w obszarze bezpieczeństwa poczty elektronicznej (np. Gartner, Forrester Wave, Frost Radar).
2	Podstawowe moduły zabezpieczające (warstwa bramy pocztowej) muszą być możliwe do wdrożenia w modelu lokalnym (on-premise) w infrastrukturze Zamawiającego; zaawansowane funkcje analizy zagrożeń (analiza załączników w środowisku sandbox oraz analiza i ochrona adresów URL) mogą być świadczone jako usługi chmurowe producenta, zgodnie z wymaganiami dotyczącymi lokalizacji przetwarzania danych określonymi w Sekcji IV.
3	Rozwiązanie musi udostępniać narzędzia lub interfejs programistyczny (API) umożliwiający integrację z rozwiązaniami bezpieczeństwa innych producentów w celu rozszerzenia funkcjonalności.
4	Rozwiązanie musi umożliwiać szybką i bezproblemową konfigurację bez konieczności zmiany rekordów MX, a także — alternatywnie — wdrożenie w oparciu o rekordy MX.
5	Rozwiązanie musi zapewniać wdrożenie i stałe monitorowanie DMARC oraz umożliwiać świadczenie usług powiązanych, takich jak archiwizacja wiadomości e-mail i usługi ciągłości działania.
6	Wykonawca, w przypadku wykupienia dodatkowej usługi serwisowej wykraczającej poza wsparcie producenta, musi zapewnić wsparcie co najmniej w godzinach pracy Zamawiającego. Godziny pracy Urzędu Miejskiego w Gliwicach są dostępne na stronie internetowej Urzędu: bip.gliwice.eu .
7	Rozwiązanie musi udostępniać konfigurowalny portal zarządzania z kontrolą dostępu opartą na rolach (RBAC), dostosowaną do uprawnień i wymagań użytkownika.
8	Rozwiązanie musi zapewniać zdefiniowaną, regularną częstotliwość aktualizacji i poprawek platformy bezpieczeństwa poczty elektronicznej (Wykonawca wskaże częstotliwość: miesięczna / kwartalna / roczna).

Lp.	Wymaganie minimalne
9	Rozwiązanie musi obsługiwać synchronizację użytkowników i grup zarówno z lokalną usługą katalogową Active Directory (poprzez mechanizm push lub protokół LDAPS), jak i z usługą Azure AD / Microsoft Entra ID lub równoważną.
10	Rozwiązanie musi umożliwiać integrację ze standardem SAML 2.0 w celu uwierzytelniania i bezpiecznego dostępu.
11	Rozwiązanie musi zapewniać mechanizm jednokrotnego logowania (SSO) z usługą katalogową lub mechanizm synchronizacji haseł, umożliwiający użytkownikom korzystanie ze standardowych poświadczeń domenowych.
12	Rozwiązanie musi umożliwiać ograniczenie dostępu do portalu administracyjnego na podstawie określonych adresów IP.
13	Rozwiązanie musi umożliwiać przydzielenie dedykowanych, statycznych, publicznych adresów IP wyłącznie dla Zamawiającego (nieudostępnianych innym podmiotom) — zarówno dla ruchu wychodzącego, jak i przychodzącego.
14	Rozwiązanie musi udostępniać interfejs administracyjny umożliwiający skuteczne śledzenie przepływu wiadomości e-mail (message tracking) oraz monitorowanie i analizę transakcji pocztowych.
15	Wykonawca musi udostępnić na żądanie środowisko testowe UAT (User Acceptance Testing) umożliwiające przetestowanie i walidację rozwiązania.
16	Rozwiązanie musi integrować się z lokalnym serwerem poczty elektronicznej Zamawiającego oraz pakietem biurowym eksploatowanym przez Zamawiającego (lub środowiskiem równoważnym), zapewniając łatwe wdrożenie i zarządzanie.
17	Rozwiązanie musi udostępniać interfejs zarządzania politykami umożliwiający konfigurowanie złożonych, zagnieżdżonych reguł dla ruchu przychodzącego i wychodzącego.
18	Rozwiązanie musi udostępniać interfejs zarządzania politykami z możliwością kwarantanny wiadomości na podstawie zdefiniowanych reguł, z możliwością przekierowania wiadomości do administratora/SOC i ich późniejszego zwolnienia do użytkowników.
19	Rozwiązanie musi obsługiwać wymuszony protokół TLS w wersji co najmniej 1.2 dla ruchu przychodzącego i wychodzącego.
20	Rozwiązanie musi szyfrować dane przechowywane (w spoczynku) — w tym przechowywane wiadomości, kwarantannę oraz dzienniki zdarzeń — a także dane przesyłane (w trakcie transmisji).
21	Rozwiązanie musi integrować się z lokalnymi bramami pocztowymi poprzez przekazywanie wiadomości za pośrednictwem agenta MTA (relay).
22	Rozwiązanie musi obsługiwać zarówno odbieranie poczty przychodzącej, jak i wysyłanie poczty wychodzącej, pełniąc rolę bramy / agenta MTA dla obu kierunków przepływu poczty.
23	Rozwiązanie musi obsługiwać wiele domen pocztowych Zamawiającego — zarówno przy odbieraniu, jak i wysyłaniu poczty — bez dodatkowych opłat licencyjnych uzależnionych od liczby obsługiwanych domen.
24	Rozwiązanie musi umożliwiać przechowywanie kopii wiadomości e-mail w pierwszym punkcie wejścia przez ograniczony czas, na potrzeby analizy i dochodzeń kryminalistycznych (zapewnienie wiarygodnego, dostępnego źródła danych do analizy).

2. Ochrona przed przejęciem biznesowej poczty e-mail (BEC)

Sztuczna inteligencja / uczenie maszynowe, analiza behawioralna i reputacyjna

Lp.	Wymaganie minimalne
25	Rozwiązanie musi skutecznie blokować ataki realizowane za pośrednictwem poczty e-mail, w tym Business Email Compromise (BEC), złośliwe oprogramowanie, phishing oraz przejęcie konta poczty e-mail (EAC).

Lp.	Wymaganie minimalne
26	Rozwiązanie musi wykorzystywać technologię antyphishingową opartą na AI/ML do wykrywania wzorców komunikacji i anomalii w stylu konwersacji oraz analizę obrazu (computer vision) do badania podejrzanych adresów URL, zapewniając ukierunkowaną ochronę przed atakami BEC.
27	Rozwiązanie musi dynamicznie analizować zawartość nagłówków oraz treści wiadomości w celu wykrywania ataków polegających na podszywaniu się pod domenę, podszywaniu się pod nazwę wyświetlaną oraz rejestracji domen łudząco podobnych (typosquatting).
28	Rozwiązanie musi zawierać klasyfikator wykrywający oszustów (impostor), wykorzystujący złożoną ocenę spamu i uczenie maszynowe do rozpoznawania wzorców ruchu pocztowego organizacji oraz proaktywnej ochrony przed atakami BEC.
29	Rozwiązanie musi zapewniać analizę łańcucha dostaw oraz łańcucha kontaktów opartą na AI/ML w celu identyfikacji i obrony przed atakami socjotechnicznymi, podszywaniem się oraz BEC.

3. Phishing, ransomware i złośliwe oprogramowanie

Sztuczna inteligencja / uczenie maszynowe, analiza behawioralna i reputacyjna; przepisywanie adresów URL i analiza w izolowanym środowisku (sandbox) w czasie kliknięcia; analiza załączników w środowisku sandbox

Lp.	Wymaganie minimalne
30	Rozwiązanie musi zapewniać kompleksową ochronę przed atakami phishingowymi, w tym zaawansowaną ochronę przed phishingiem, wykrywanie oszustów oraz ochronę poczty wewnętrznej.
31	Rozwiązanie musi proaktywnie analizować podejrzane adresy URL w środowisku sandbox z użyciem analizy dynamicznej/behawioralnej, aby zapobiegać rozprzestrzenianiu się złośliwego oprogramowania i innych zagrożeń.
32	Rozwiązanie musi blokować złośliwe adresy URL, wykorzystywać przepisywanie adresów URL oraz udostępniać konfigurowalne strony blokady dla niebezpiecznych witryn (edukacja użytkowników).
33	Rozwiązanie musi wykorzystywać technologie AI/ML w celu zwiększenia skuteczności wykrywania zagrożeń w poczcie elektronicznej.
34	Rozwiązanie musi wykorzystywać AI/ML do analizy wzorców komunikacji w celu zapobiegania przychodzącemu phishingowi oraz wykrywania potencjalnie błędnie zaadresowanych wiadomości.
35	Rozwiązanie musi umożliwiać tworzenie niestandardowych reguł antyphishingowych oraz analizę AI/ML do wykrywania ukierunkowanych ataków phishingowych o niskiej skali.
36	Rozwiązanie musi zapewniać integrację API z platformami współpracy w celu filtrowania złośliwych treści lub podejrzanych interakcji.
37	Rozwiązanie musi zapewniać ochronę przed atakami DoS oraz zbieraniem katalogów (directory harvesting) w celu zachowania dostępności usług poczty.
38	Rozwiązanie musi zapewniać ochronę przed atakami wykradającymi poświadczenia (wiadomości phishingowe kierujące do fałszywych stron logowania).
39	Rozwiązanie musi zapewniać ochronę przed spear-phishingiem, w szczególności przed opóźnionymi exploitami.
40	Rozwiązanie musi być zdolne do przeprowadzania analizy z wykorzystaniem technik przeciwdziałających uchylaniu się od wykrycia (anti-evasion).
41	Rozwiązanie musi obsługiwać przepisywanie adresów URL dla wiadomości przychodzących, zapewniając bezpieczne wykonanie za pośrednictwem platformy izolacji.
42	Rozwiązanie musi przeprowadzać inspekcję adresów URL w czasie rzeczywistym w treści wiadomości, załącznikach (PDF, dokumenty pakietu biurowego itp.) oraz w serwisach udostępniania plików (np. OneDrive, SharePoint lub równoważnych).

Lp.	Wymaganie minimalne
43	Rozwiązanie musi wykorzystywać analizę obrazu AI/ML do wykrywania i blokowania złośliwych adresów URL.
44	Rozwiązanie musi blokować adresy URL na podstawie reputacji jeszcze przed dostarczeniem, z wykorzystaniem analizy predykcyjnej.
45	Rozwiązanie musi obsługiwać ochronę adresów URL po dostarczeniu (np. analizę zawartości adresu URL w sandbox).
46	Rozwiązanie musi stale i wstecznie analizować złośliwe adresy URL po dostarczeniu oraz umożliwiać administratorom usuwanie wiadomości, których dotyczy problem (monitorowanie zachowania adresu URL pod kątem opóźnionych ataków).
47	Rozwiązanie musi umożliwiać weryfikację adresów URL w wiadomościach na podstawie czasu kliknięcia (time-of-click).
48	Rozwiązanie musi zapewniać izolowane środowiska kontenerowe (tylko do odczytu) do wykonywania podejrzanych adresów URL i linków w wiadomościach lub załącznikach.
49	Rozwiązanie musi umożliwiać dekodowanie przepisanych adresów URL w celu identyfikacji oryginalnej witryny docelowej.
50	Rozwiązanie musi utrzymywać dostarczanie wiadomości w trakcie analizy wszystkich adresów URL i linków zawartych w wiadomości.
51	Rozwiązanie musi umożliwiać administratorom nadpisywanie blokad adresów URL i podejmowanie świadomych decyzji o zezwoleniu.
52	Rozwiązanie musi umożliwiać izolację stron internetowych i wymuszać tryb tylko do odczytu, aby zapobiec nieautoryzowanemu przesyłaniu poświadczeń i danych użytkownika.
53	Rozwiązanie musi bezpiecznie przechowywać dane wiadomości i załączników na platformie izolacji.
54	Rozwiązanie musi realizować analizę typu sandbox (detonację) załączników w środowisku zlokalizowanym wyłącznie na terenie EOG — lokalnie w infrastrukturze Zamawiającego lub w chmurze prywatnej/publicznej w regionie EOG; dane załączników nie mogą być przekazywane poza EOG (zob. Sekcja IV).

4. Raportowanie i korygowanie wiadomości e-mail

Zautomatyzowana orkiestracja i reagowanie na incydenty (mSOAR); automatyczna obsługa skrzynki zgłoszeń nadużyć; zgłaszanie podejrzanych wiadomości przez użytkowników

Lp.	Wymaganie minimalne
55	Rozwiązanie musi umożliwiać połączenie ze skrzynką nadużyć (abuse mailbox) i automatyzację usuwania wiadomości wysłanych do tej skrzynki.
56	Rozwiązanie musi obsługiwać API umożliwiające integrację zdarzeń poczty z systemami XDR, SIEM oraz mSOAR.
57	Rozwiązanie musi obsługiwać zautomatyzowane korygowanie dostarczonych zagrożeń.
58	Rozwiązanie musi umożliwiać administratorom analizowanie i przenoszenie złośliwych lub niechcianych wiadomości do kwarantanny po dostarczeniu.
59	Rozwiązanie musi wykrywać i usuwać złośliwe wiadomości przekazane wewnętrznie.
60	Rozwiązanie musi zapewniać mechanizm ręcznego przeglądu wiadomości z możliwością śledzenia działań użytkownika.
61	Rozwiązanie musi obsługiwać ręczne usuwanie wiadomości ze skrzynek z wykorzystaniem formatu pliku JSON.
62	Rozwiązanie musi konsolidować alerty z wielu źródeł i korelować je w jedno zdarzenie.

Lp.	Wymaganie minimalne
63	Rozwiązanie musi wykorzystywać informacje o zagrożeniach (threat intelligence) z różnych źródeł i automatycznie wzbogacać alerty.
64	Rozwiązanie musi zapewniać automatyczną kwarantannę i powstrzymywanie zagrożeń lub proste działania ochronne dla szybkiej reakcji.
65	Rozwiązanie musi automatyzować zarządzanie użytkownikami, wiadomościami, hostami, adresami IP i URL w systemach egzekwowania podczas ataku.
66	Rozwiązanie musi udostępniać banery kontekstowe ostrzegające użytkowników oraz przycisk zgłaszania wiadomości nie wymagający instalacji.
67	Rozwiązanie musi wyświetlać banery HTML w klientach poczty, automatycznie przełączając się na format zwykłego tekstu, gdy HTML nie jest obsługiwany, z obsługą wielu języków i możliwością edycji treści banera przez organizację.
68	Rozwiązanie musi automatycznie analizować wiadomości zgłoszone przez użytkowników w celu weryfikacji ich złośliwego charakteru.
69	Rozwiązanie musi integrować się z narzędziami mSOAR w celu automatyzacji procesu zgłaszania złośliwych wiadomości, w tym ich przeklasyfikowania i usuwania ze skrzynek.
70	Rozwiązanie musi umożliwiać dodanie szyfrowania do wiadomości w celu zapobiegania nieautoryzowanemu dostępowi do treści.
71	Rozwiązanie musi analizować treść wiadomości i umożliwiać blokowanie, przekierowanie lub szyfrowanie wiadomości na podstawie tej analizy.
72	Rozwiązanie musi umożliwiać zabezpieczanie, śledzenie i ewentualną redakcję poufnych danych udostępnianych w wiadomościach partnerom i klientom.
73	Rozwiązanie musi oferować wiele opcji obsługi zagrożeń, w tym usuwanie załączników, powiadamianie nadawców oraz kwarantannę całej wiadomości.
74	Rozwiązanie musi udostępniać administratorom funkcję „Bezpieczny podgląd” do wyświetlania szczegółów wiadomości w kwarantannie i podejmowania decyzji o niezbędnych akcjach.
75	Rozwiązanie musi umożliwiać użytkownikom końcowym zgłaszanie wyników fałszywie ujemnych i fałszywie dodatnich.
76	Rozwiązanie musi automatycznie usuwać/wycofywać wszystkie wiadomości uznane za złośliwe po dostarczeniu.
77	Rozwiązanie musi pozyskiwać wiadomości zgłaszane przez użytkowników z różnych źródeł, w tym ze skrzynki nadużyć, dodatku do klienta poczty oraz dynamicznych banerów HTML.
78	Rozwiązanie musi automatyzować reakcje przy użyciu predefiniowanych zestawów reguł lub playbooków dla różnych zadań, w tym badania alertów, oceny wpływu i działań naprawczych.
79	Rozwiązanie musi automatyzować reakcje na wiadomości przekazane oraz podobne wiadomości dostarczone użytkownikom, w szczególności gdy zostaną zidentyfikowane jako złośliwe.
80	Rozwiązanie musi umożliwiać przypisywanie poziomów ważności lub ocen wykrytym zagrożeniom, umożliwiając skuteczną priorytetyzację i alokację zasobów.
81	Rozwiązanie musi udostępniać kompleksowy portal umożliwiający dostęp do informacji i metadanych o zdarzeniach/incydentach na potrzeby analizy zagrożeń.
82	Rozwiązanie musi umożliwiać zespołom bezpieczeństwa i osobom reagującym na incydenty automatyzację identyfikacji, korygowania i udostępniania zagrożeń phishingowych.
83	Rozwiązanie musi przekazywać użytkownikom informacje zwrotne w zależności od typu zgłaszanej wiadomości, umożliwiając zamykanie zgłoszeń i oferując terminowe aktualizacje lub rozwiązania.
84	Rozwiązanie musi zapewniać osobom reagującym na incydenty analizę w czasie rzeczywistym oraz wgląd w ataki pocztowe wymierzone w organizację.

5. Pulpity nawigacyjne oraz raporty o zagrożeniach i użytkownikach

Szczegółowe informacje o zagrożeniach (w tym identyfikacja osób szczególnie narażonych na ataki — VAP); pulpit oceny ryzyka użytkowników

Lp.	Wymaganie minimalne
85	Rozwiązanie musi zapewniać widoczność zagrożeń bezpieczeństwa w organizacji, w tym: najczęściej atakowane konta e-mail, sposób ataku na te konta, użytkowników o zachowaniach wysokiego ryzyka oraz sposób uzyskiwania przez nich dostępu do danych.
86	Rozwiązanie musi dostarczać raport podsumowujący dla kadry zarządzającej, obejmujący m.in.: filtry czasowe, liczbę wiadomości przychodzących/wychodzących, spam, wiadomości masowe, phishing, wiadomości złośliwe (AV, antymalware, sandbox), najczęstsze złośliwe adresy URL i złe domeny oraz ataki ukierunkowane z wybranego obszaru geograficznego.
87	Rozwiązanie musi umożliwiać segmentację/filtrowanie danych raportowych wg kryteriów, np. kraju, hierarchii organizacyjnej, jednostek biznesowych, działów, opisu stanowiska oraz typu wektora ataku (spam, malware, phishing, złośliwe adresy URL, złe domeny).
88	Rozwiązanie musi zapewniać szczegółową, bogatą w kontekst i umożliwiającą podejmowanie działań analizę zagrożeń, w tym wskaźniki naruszenia bezpieczeństwa (IOC) oraz informacje o odbiorcach.
89	Wykonawca powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.
90	Rozwiązanie musi zapewniać szczegółowe raporty obejmujące użycie systemu (globalne podsumowanie wiadomości, spam, wirusy, działania reguł) z możliwością wysyłki e-mail (HTML), druku lub pobrania w formacie CSV.
91	Rozwiązanie musi umożliwiać administratorom wyświetlanie raportów ze szczegółowymi statystykami przetworzonych i odrzuconych wiadomości, transakcji SMTP oraz przepływów komunikacji.
92	Rozwiązanie musi umożliwiać porównanie liczby i dotkliwości ataków z innymi organizacjami z branży lub grupami porównawczymi.
93	Rozwiązanie musi dostarczać informacje o podmiotach (aktorach) atakujących organizację.
94	Rozwiązanie musi rozpoznawać, czy wiadomości stanowią część kampanii ukierunkowanej na organizację.
95	Rozwiązanie musi udostępniać administratorom zaawansowane pulpity zagrożeń zawierające trendy i analizy malware/spamu, analizę sandbox, kliknięcia adresów URL oraz próby phishingu.
96	Rozwiązanie musi zawierać raporty o zamiarach atakujących (np. malware, kradzież poświadczeń, podszywanie się) oraz próbach ransomware (np. broker dostępu pocztowego).
97	Rozwiązanie musi zapewniać szczegółowe raportowanie liczby i typów wiadomości zgłaszanych przez użytkowników oraz rozumienie trendów ataków wpływających na organizację.
98	Rozwiązanie musi dostarczać szczegółowe informacje oparte na ryzyku oraz rekomendować kontrolę zabezpieczeń na podstawie tych informacji.
99	Rozwiązanie musi zapewniać eksport danych przez API w celu integracji z SOC.
100	Rozwiązanie musi umożliwiać administratorom szybkie generowanie raportów w czasie rzeczywistym w interfejsie zarządzania.
101	Rozwiązanie musi umożliwiać monitorowanie i porównywanie z innymi firmami z branży w ujęciu pionowym (benchmark).
102	Rozwiązanie musi obsługiwać pełną inspekcję wiadomości przychodzących i wychodzących.
103	Rozwiązanie musi zapewniać prostotę oceny oraz dodatkowy wgląd w ruch wewnętrzny i inne kanały komunikacji, a także w aktywność wychodzącą użytkowników w celu wykrywania podejrzanych zachowań.
104	Rozwiązanie musi zapewniać praktyczny pulpit zagrożeń umożliwiający tworzenie usprawnionych przepływów pracy do szybkiego reagowania na zagrożenia związane z malware/wirusami przesyłanymi pocztą.

6. Higiena i konfiguracja poczty przychodzącej

Ochrona przed spamem i wirusami, filtrowanie niechcianych wiadomości masowych (newslettery, powiadomienia marketingowe — tzw. graymail), szczególna ochrona kadry kierowniczej i osób na kluczowych stanowiskach (VIP) oraz możliwość dostosowywania reguł i polityk bezpieczeństwa

Lp.	Wymaganie minimalne
105	Rozwiązanie musi obsługiwać dokładne wykrywanie i blokowanie złośliwych wiadomości z wykorzystaniem automatycznej analizy malware, w tym: blokowanie wiadomości od znanych nieprawidłowych nadawców, skanowanie załączników programem antywirusowym, blokowanie wiadomości ze znanymi złośliwymi adresami URL oraz analizę treści w celu identyfikacji spamu.
106	Rozwiązanie musi posiadać zaawansowane możliwości ochrony, w tym: przepisywanie adresów URL, skanowanie antywirusowe, integrację z sandbox, kwarantannę spamu z podsumowaniami dla użytkowników końcowych, obsługę niechcianych wiadomości masowych (tzw. graymail), ochronę BEC oraz wycofanie po dostarczeniu.
107	Rozwiązanie musi charakteryzować się wysoką skutecznością w wykrywaniu spamu.
108	Rozwiązanie musi zapewniać wysoką dostępność usług, odpowiadającą potrzebom biznesowym Zamawiającego.
109	Rozwiązanie musi zapewniać pełną ochronę przed znanymi zagrożeniami ze strony złośliwego oprogramowania.
110	Rozwiązanie musi utrzymywać niski wskaźnik wyników fałszywie dodatnich przy jednoczesnym skutecznym identyfikowaniu i blokowaniu złośliwej zawartości.
111	Rozwiązanie musi zapewniać niskie opóźnienia w dostarczaniu poczty.
112	Rozwiązanie musi skutecznie i terminowo skanować oraz zwalniać załączniki.
113	Rozwiązanie musi umożliwiać terminową identyfikację i śledzenie wiadomości po ich wysłaniu.
114	Rozwiązanie musi obsługiwać zarządzanie klasyfikacją wiadomości, w tym oddzielne klasyfikatory dla spamu, podszywania się, wiadomości masowych, phishingu, treści dla dorosłych i malware, z możliwością ustawiania progów punktacji dla każdej kategorii.
115	Rozwiązanie musi obsługiwać skanowanie i stosowanie reguł dla plików zaszyfrowanych lub chronionych hasłem oraz wielokrotnie skompresowanych.
116	Rozwiązanie musi obsługiwać precyzyjne dostrajanie poziomu wykrywania spamu.
117	Rozwiązanie musi obsługiwać wykrywanie nowych kampanii spamowych.
118	Rozwiązanie musi automatycznie usuwać podejrzaną wiadomości ze skrzynek odbiorczych użytkowników.
119	Rozwiązanie musi zapewniać szczegółowe mechanizmy kontroli administracyjnej z dostępem opartym na rolach do każdego modułu i folderu kwarantanny.
120	Rozwiązanie musi zezwalać użytkownikowi końcowemu na dostęp do niezłośliwych wiadomości w kwarantannie, jednocześnie uniemożliwiając dostęp do wiadomości złośliwych.
121	Rozwiązanie musi spełniać złożone wymagania dotyczące routingu poczty, w tym routingu opartego na grupach użytkowników.
122	Rozwiązanie musi korzystać z zaawansowanych technik ochrony przed kradzieżą poświadczeń oraz analizy obrazu w celu wykrywania i blokowania ataków phishingowych podszywających się pod strony logowania.
123	Rozwiązanie musi wykorzystywać uczenie maszynowe do ciągłego monitorowania i dostosowywania się do wzorców komunikacji e-mail w organizacji.
124	Rozwiązanie musi generować logi w widoku zbliżonym do czasu rzeczywistego oraz oferować wydajne wyszukiwanie danych dziennika z zaawansowanymi filtrami.
125	Rozwiązanie musi obsługiwać integrację z zewnętrznymi magazynami danych i bazami danych.

Lp.	Wymaganie minimalne
126	Rozwiązanie musi zapewniać skuteczne wykrywanie spamu w wielu językach, w tym m.in. chińskim (uproszczonym i tradycyjnym), angielskim, japońskim, koreańskim, tajskim i wietnamskim.
127	Rozwiązanie musi umożliwiać administratorom przypisywanie różnych zestawów reguł na podstawie określonych adresów e-mail.
128	Rozwiązanie musi oferować weryfikację odbiorcy w usłudze katalogowej oraz innych źródłach list e-mail, aby zapobiegać spoofingowi i usprawniać dostarczanie wiadomości.
129	Rozwiązanie musi obsługiwać szeroki zakres zachowań i akcji routingu dla różnych scenariuszy obsługi poczty.
130	Rozwiązanie musi umożliwiać zarządzanie stopkami w wiadomościach przychodzących i wychodzących, w tym: wstawianie stopek prawnych i zgodności (np. klauzul poufności), obsługę wielu języków, stosowanie filtrów na podstawie atrybutów wiadomości lub Active Directory, wstawianie treści dynamicznej (np. daty), warunkowe stosowanie w określonych przeskokach routingu, selektywne stosowanie na podstawie polityki/attributu, pomijanie dla wiadomości szyfrowanych S/MIME lub podpisanych cyfrowo oraz stosowanie podpisów i zastrzeżeń na podstawie grup użytkowników AD.
131	Rozwiązanie musi umożliwiać użytkownikom końcowym otrzymywanie niestandardowych powiadomień e-mail na podstawie nazwy domeny.
132	Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe dla użytkowników końcowych, administratorów platformy i administratorów systemu.
133	Rozwiązanie musi zapewniać internetową konsolę zarządzania i konfiguracji centralizującą konfigurację, rejestrowanie, kwarantannę i raportowanie, kompatybilną z nowoczesnymi przeglądarkami.
134	Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach do konsoli zarządzania, z możliwością przypisania nazwanym kontom administratorów określonych uprawnień; konsola musi obsługiwać usługę katalogową i uwierzytelnianie wieloskładnikowe.
135	Rozwiązanie musi zapewniać administratorom możliwość zarządzania kolejką poczty e-mail.
136	Rozwiązanie musi umożliwiać delegowanie administracji do podorganizacji w oparciu o logiczne grupowania użytkowników (jednostki biznesowe, regiony, role, funkcje, hierarchia), z dziedziczeniem zasad z organizacji głównej oraz możliwością ich nadpisywania.
137	Rozwiązanie musi obsługiwać powiadamianie zespołu bezpieczeństwa o wszystkich zasadach, folderach kwarantanny i progach kolejki.
138	Rozwiązanie musi umożliwiać ograniczenie rozmiaru wysyłanych/odbieranych wiadomości lub liczby adresatów.
139	Rozwiązanie musi umożliwiać ograniczenie sondowania SMTP oraz walidację informacji na kopercie przed przyjęciem wiadomości do dostarczenia.
140	Rozwiązanie musi zapewniać narzędzia do diagnozowania problemów z routingiem aplikacji i wiadomości, z możliwością śledzenia wiadomości (message trace) wspierającą pomoc techniczną.
141	Rozwiązanie musi umożliwiać dołączanie słów kluczowych do tematu, nagłówka i treści wiadomości na podstawie zestawu reguł.
142	Rozwiązanie musi obsługiwać tworzenie list bezpiecznych/zablokowanych na podstawie użytkowników lub grup użytkowników.
143	Rozwiązanie musi obsługiwać importowanie wielu użytkowników/grup do list bezpiecznych/zablokowanych z plików CSV/tekstowych.
144	Rozwiązanie musi obsługiwać i filtrować biuletyny informacyjne oraz masowy spam.
145	Rozwiązanie musi wykrywać ataki spamowe oparte na tekście, obrazach, multimediami i załącznikach.
146	Rozwiązanie musi obsługiwać ukierunkowane blokowanie wiadomości spamowych.
147	Rozwiązanie musi wykrywać kampanie spamowe i dodawać ich źródło do czarnej listy, natychmiast blokując połączenia z danego serwera pocztowego.

Lp.	Wymaganie minimalne
148	Rozwiązanie musi zapewniać ochronę przed nękaniami pocztą i ograniczać ryzyko związane z wiadomościami od nieznanymi nadawców, szczególnie dla kadry kierowniczej i VIP.
149	Rozwiązanie musi oferować możliwości analizy fałszerstw (spoofing) podszywających się pod domeny biznesowe.
150	Rozwiązanie musi obsługiwać filtrowanie połączeń w oparciu o reputację (domeny lub adresy IP).
151	Rozwiązanie musi integrować się z zewnętrznymi silnikami antywirusowymi i antymalware w celu filtrowania wiadomości.
152	Rozwiązanie musi umożliwiać blokowanie określonych typów plików na podstawie rozszerzeń (np. .exe, .dll, .doc/.docx, .xls/.xlsx, .ppt/.pptx, .jpg, .png, .pdf, .swf, .mp3/.mp4, .java, .vbs).
153	Rozwiązanie musi umożliwiać blokowanie archiwów załączników (np. .zip, .tgz, .7z, .cab, .lzh, .rar, .tnef).

7. Obsługa DMARC w systemie ochrony poczty

Weryfikacja i egzekwowanie mechanizmów uwierzytelniania poczty (SPF, DKIM, DMARC)

Lp.	Wymaganie minimalne
154	Weryfikacja i egzekwowanie DMARC (ruch przychodzący). System musi zapewniać weryfikację wiadomości przychodzących w oparciu o mechanizmy SPF, DKIM i DMARC, sprawdzanie zgodności (alignment) domen pomiędzy nagłówkami SPF/DKIM a domeną nadawcy, identyfikację statusu DMARC (pass/fail/none) oraz wykorzystanie wyniku DMARC jako warunku w politykach bezpieczeństwa.
155	Polityki bezpieczeństwa oparte o DMARC. System musi umożliwiać definiowanie granularnych polityk przetwarzania wiadomości w oparciu o wynik DMARC, w tym: kwarantannę wiadomości niespełniających DMARC, odrzucenie wiadomości (reject), oznaczanie/tagowanie (np. modyfikacja tematu lub nagłówków) oraz przepuszczanie wiadomości (allow) w uzasadnionych przypadkach; musi umożliwiać łączenie wyniku DMARC z dodatkowymi warunkami (grupy użytkowników, VIP, inne sygnały) oraz definiowanie wyjątków (zaufani nadawcy, scenariusze forwardingu).
156	Tryb monitorowania (non-blocking). System musi umożliwiać wdrożenie polityk DMARC w trybie monitorowania (bez blokowania ruchu) oraz stopniowe zaostrzanie polityk (od monitorowania, przez kwarantannę, po odrzucanie).
157	Wsparcie dla mechanizmów uwierzytelniania (DMARC readiness). System musi wspierać konfigurację i obsługę podpisywania DKIM dla wiadomości wychodzących, w tym obsługę odrębnych kluczy i selektorów DKIM dla różnych domen nadawczych (obsługa wielu domen), integrację z istniejącą konfiguracją SPF po stronie Zamawiającego oraz obsługę wielu domen nadawczych.
158	System musi obsługiwać zachowanie wyników uwierzytelniania wiadomości (SPF, DKIM, DMARC) przy przekazywaniu poczty przez serwery pośredniczące, na przykład przekierowania i listy dystrybucyjne (standard ARC), tak aby prawidłowo uwierzytelnione wiadomości nie były błędnie odrzucane po przejściu przez takie systemy.
159	Widoczność i logowanie. System musi zapewniać widoczność wyników SPF, DKIM i DMARC dla przetwarzanych wiadomości, dostęp do logów umożliwiających analizę decyzji podjętych na podstawie DMARC, wyszukiwanie i filtrowanie wiadomości na podstawie statusu DMARC oraz wykorzystanie danych DMARC w raportach operacyjnych.
160	Integracja z silnikiem polityk bezpieczeństwa. System musi umożliwiać wykorzystanie wyników DMARC jako jednego z wielu sygnałów w silniku decyzyjnym oraz wspierać centralne zarządzanie politykami bezpieczeństwa dla poczty przychodzącej.

8. Zapobieganie utracie danych (DLP)

Wbudowane reguły ochrony; rozpoznawanie danych wrażliwych metodą cyfrowych odcisków (fingerprinting); mechanizm samodzielnej korekty błędów przez użytkownika (np. ostrzeżenie o błędnym adresacie przed wysłaniem)

Lp.	Wymaganie minimalne
161	Rozwiązanie musi zawierać funkcje zapobiegania utracie danych (DLP) w wiadomościach e-mail, aby przeciwdziałać nieautoryzowanemu przesyłaniu danych poufnych lub danych osobowych (PII), z możliwością blokowania lub zgłaszania takich transmisji.
162	Rozwiązanie musi obsługiwać bezpieczne opcje szyfrowania wiadomości, w tym TLS oraz szyfrowanie push/pull, w celu ochrony poufnych informacji podczas przesyłania.
163	Rozwiązanie musi umożliwiać bezpieczne wysyłanie dużych plików za pośrednictwem portalu zintegrowanego z rozwiązaniem do szyfrowania poczty.
164	Rozwiązanie musi zapewniać powiadomienia i alerty w czasie rzeczywistym dotyczące naruszeń zasad lub podejrzanych działań związanych z DLP.

VI. Wdrożenie

W ramach usług wdrożeniowych Wykonawca zobowiązany jest w szczególności do:

- opracowania i uzgodnienia z Zamawiającym szczegółowego harmonogramu i planu wdrożenia, w tym spotkania inicjującego (kick-off) oraz planu testów;
- dostarczenia obrazu maszyny wirtualnej (OVA/OVF) oraz instalację i konfigurację warstwy lokalnej (on-premise) w środowisku VMware vSphere 8 Zamawiającego;
- konfiguracji modułów zabezpieczających oraz polityk bezpieczeństwa dla poczty przychodzącej i wychodzącej (antyspam, antywirus, antyphishing, ochrona przed BEC, DLP, kwarantanna, routing);
- konfiguracji uwierzytelniania poczty: weryfikacji SPF, DKIM i DMARC dla poczty przychodzącej oraz podpisywania DKIM dla poczty wychodzącej, w tym osobnych kluczy i selektorów dla różnych domen;
- integracji z usługą katalogową (synchronizacja użytkowników i grup), serwerem poczty (Exchange / Microsoft 365 lub równoważnym) oraz mechanizmami uwierzytelniania (SSO / SAML 2.0);
- konfiguracji i powiązania usług chmurowych (analiza załączników w środowisku sandbox z rezydencją danych w EOG oraz analiza i ochrona adresów URL) z warstwą lokalną;
- konfiguracji przepływu i routingu poczty oraz produkcyjne przełączenie (cutover) ruchu przychodzącego i wychodzącego, z opcją bez zmiany rekordów MX oraz w oparciu o rekordy MX;
- przeprowadzenia testów akceptacyjnych (ang. User Acceptance Testing, dalej „UAT”) według uzgodnionego planu testów oraz walidację poprawnego działania Systemu;
- stabilizację powdrożeniową oraz korektę konfiguracji w zakresie ujawnionym podczas testów i po przełączeniu produkcyjnym;
- przekazania wiedzy (instruktaż) administratorom Zamawiającego oraz dostarczenie dokumentacji powykonawczej;
- zapewnienia wsparcia powdrożeniowego w uzgodnionym okresie stabilizacji.

VII. Wsparcie techniczne i serwis

Przez „podwyższony poziom wsparcia” Zamawiający rozumie wsparcie techniczne świadczone przez producenta rozwiązania (lub podmiot autoryzowany przez producenta) o parametrach nie gorszych niż określone w niniejszej sekcji. Występujące na rynku nazwy handlowe takich poziomów (np. „Platinum”, „Premium”, „Premier”) służą wyłącznie zilustrowaniu oczekiwanego poziomu. Wymagany poziom wsparcia obejmuje co najmniej:

1. wsparcie techniczne producenta (lub podmiotu autoryzowanego) przez cały 12-miesięczny okres obowiązywania umowy, w trybie zapewniającym całodobową (24×7) obsługę zgłoszeń krytycznych;
2. klasyfikację zgłoszeń według priorytetów oraz gwarantowane (docelowe) czasy reakcji nie gorsze niż określone w poniższej tabeli:

Priorytet	Opis zgłoszenia	Tryb obsługi	Maks. czas reakcji
P1 — krytyczny	System niedziałający lub brak przepływu poczty; brak obejścia, krytyczny wpływ na działalność	24×7	1 godzina
P2 — wysoki	Poważne ograniczenie funkcjonalności; dostępne obejście	godziny robocze	4 godziny robocze
P3 — standardowy	Pomniejszy problem, pytanie lub wniosek o zmianę	godziny robocze	8 godzin roboczych

Czas reakcji oznacza czas od przyjęcia zgłoszenia do podjęcia działań przez wsparcie. Czasy reakcji dla zgłoszeń P2–P3 liczone są w godzinach roboczych Zamawiającego.

3. co najmniej cztery (4) imienne (autoryzowane) osoby kontaktowe po stronie Zamawiającego uprawnione do zgłaszania i obsługi zgłoszeń u producenta;
4. kanały zgłaszania incydentów i awarii: portal serwisowy producenta z możliwością śledzenia statusu zgłoszeń, poczta elektroniczna oraz telefon (kanał telefoniczny dostępny dla zgłoszeń krytycznych);
5. dostęp do aktualizacji i poprawek oprogramowania (w tym aktualizacji sygnatur i mechanizmów detekcji) przez cały okres umowy;
6. wsparcie świadczone bezpośrednio przez Wykonawcę (poza wsparciem producenta) dostępne co najmniej w godzinach pracy Zamawiającego, w języku polskim lub angielskim;
7. zgodnie z wcześniejszymi postanowieniami, zakres i koszt wsparcia nie mogą być uzależnione od liczby uruchomionych instancji / agentów wirtualnych, lecz wyłącznie od liczby chronionych użytkowników;
8. szczegółowe parametry SLA, w tym czasy usunięcia awarii (naprawy) zostały określone we wzorze umowy (zgodnie z § 12).

VIII. Równoważność (klauszula równoważności)

Zgodnie z art. 99 ust. 5 i 6, art. 101 ust. 4 oraz art. 101 ust. 5–6 ustawy Pzp, Zamawiający informuje, że:

- wszędzie tam, gdzie w opisie przedmiotu zamówienia wskazano normy, oceny techniczne, specyfikacje techniczne lub systemy referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, wraz z dopiskiem „lub równoważne”;

Załącznik nr 1 do umowy

- wszędzie tam, gdzie w opisie pojawiają się nazwy własne (znaki towarowe, nazwy produktów lub technologii), służą one wyłącznie doprecyzowaniu wymagań co do parametrów i funkcjonalności lub opisaniu środowiska Zamawiającego (interoperacyjność) i należy je rozumieć z dopiskiem „lub równoważne”;
- za rozwiązanie równoważne uznaje się rozwiązanie spełniające wszystkie wymagania minimalne określone w Sekcji V niniejszego OPZ w stopniu nie gorszym niż opisany, zapewniające co najmniej tożsamy zakres funkcjonalny, poziom bezpieczeństwa, wydajność i dostępność.

IX. Gwarancja, dostępność i poziom świadczenia usług

1. Rozwiązanie musi zapewniać wysoką dostępność usługi ochrony poczty. Zamawiający oczekuje gwarantowanego poziomu dostępności warstwy oprogramowania oraz usług chmurowych (analiza załączników, analiza adresów URL) na poziomie nie niższym niż 99,9 % w skali miesiąca kalendarzowego. Dostępność komponentów wdrożonych lokalnie (on-premise) zależy również od infrastruktury teleinformatycznej Zamawiającego (m.in. środowisko wirtualizacyjne, zasilanie, sieć), w zakresie pozostającym poza kontrolą Wykonawcy. Szczegółowy sposób pomiaru dostępności, okno pomiarowe oraz wyłączenia (np. zaplanowane okna serwisowe, czynniki po stronie Zamawiającego, siła wyższa) zostały określone we wzorze umowy.
2. Rozwiązanie musi zapewniać redundancję i mechanizmy wysokiej dostępności adekwatne do wdrażanych lokalnie modułów zabezpieczających, zapewniające ciągłość filtrowania i przepływu poczty.
3. Wykonawca udzieli gwarancji na prawidłowe działanie rozwiązania oraz wykonane usługi wdrożeniowe na okres obowiązywania umowy (zgodnie z § 12 wzoru umowy).

X. Wymagania dotyczące producenta rozwiązania i bezpieczeństwa danych

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych przetwarzanych przez rozwiązanie, Zamawiający wymaga, aby producent oferowanego rozwiązania — a w przypadku usług chmurowych (analiza załączników w środowisku sandbox, analiza adresów URL) także podmiot operujący tymi usługami i przetwarzający dane Zamawiającego — posiadał ważny certyfikat ISO/IEC 27001 (System Zarządzania Bezpieczeństwem Informacji) lub równoważny, obejmujący swoim zakresem usługi oraz ośrodki przetwarzania danych istotne dla realizacji zamówienia (w tym ośrodek przetwarzania zlokalizowany na terenie EOG, w którym realizowana jest analiza załączników).

Za rozwiązanie/ certyfikat równoważny Zamawiający uzna dokument wystawiony przez niezależną jednostkę audytorską, który potwierdza wdrożenie systemu zarządzania bezpieczeństwem informacji opartego na uznanych międzynarodowych standardach. Standard równoważny musi obowiązkowo obejmować weryfikację kryteriów w obszarach: poufności, integralności i dostępności danych, zarządzania incydentami bezpieczeństwa, kontroli dostępu fizycznego i logicznego do infrastruktury EOG oraz ciągłości działania (DRP/BCP).

Jeżeli przetwarzanie danych zostaje powierzone podmiotowi trzeciemu (np. operatorowi centrum danych lub podwykonawcy przetwarzającemu dane), podmiot ten również musi posiadać certyfikat ISO/IEC 27001 lub równoważny w odpowiednim zakresie. Na potwierdzenie powyższego Wykonawca przed zawarciem umowy powierzenia przetwarzania danych osobowych przedłoży stosowny dokument (certyfikat) zgodnie z Oświadczeniem w sprawie gwarantowanych środków

technicznych i organizacyjnych stosowanych przez podmiot przetwarzający, będącym Załącznikiem nr 1 do Umowy na powierzenie przetwarzania danych osobowych.