LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA

ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup
systemu ochrony poczty elektronicznej

Spis treści

1. Słownik i skróty

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Oprogramowanie Standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące w użytkowaniu Zamawiającego.
Oprogramowanie	Oprogramowanie antywirusowe będące przedmiotem niniejszego postępowania.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Usługa Serwisu	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Oprogramowania oraz jego poszczególnych komponentów.
Użytkownik	Zamawiający oraz jego pracownicy.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający/LPR	Lotnicze Pogotowie Ratunkowe.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup systemu ochrony infrastruktury LPR: **ochrona Poczty elektronicznej.**

System ochrony komunikacji e-mail składa się z następujących elementów:

Sensory do detekcji zagrożeń w ruchu e-mail w postaci maszyn wirtualnych do obsługi 840 skrzynek pocztowych wraz ze wszystkimi wymaganymi usługami subskrypcyjnymi na okres 3 lat. Sensory są dostarczone w postaci maszyn wirtualnych w celu ograniczenia kosztów związanych z zakupem sprzętu fizycznego i jego serwisu w ilości wymaganej do obsługi 500 skrzynek pocztowych. Dołożenie kolejnego sensora w postaci wirtualnej w celu zwiększenia wydajności rozwiązania nie będzie wymagało poniesienia dodatkowych kosztów.

2.1Wymagania dotyczące systemu ochrony poczty elektronicznej (500 skrzynek pocztowych)

Kod wymagania	Opis wymagań
WPE.1	System realizuje między innymi następujące funkcje: 1) ochronę przed szkodliwą treścią (m.in. malware, wirusy, phishing etc.); 2) ochronę przed spamem; 3) filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki).
WPE.2	System pracuje jako bramka poczty elektronicznej (jako gateway MTA - Mail Transfer Agent).
WPE.3	System umożliwia kontrolę protokołów SMTP oraz ESMTP, w tym szyfrowane wersje tych protokołów z użyciem TLS.
WPE.4	System posiada specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej.
WPE.5	System zapewnia ochronę dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6.
WPE.6	System umożliwia stworzenie klastra konfiguracyjnego składające się z wielu urządzeń (fizycznych lub wirtualnych), z możliwością równoważenia obciążenia z wykorzystaniem zmian w rekordach MX DNS.

Kod wymagania	Opis wymagań
WPE.7	Konfiguracja systemu musi być możliwa przez: 1) Interfejs Web: HTTPS; 2) CLI: przez SSH; 3) API umożliwiające odczytanie z systemu co najmniej następujących informacji: a) Bieżące parametry określające status systemu, b) Zbiorowe zestawienia z określonego okresu informujące co najmniej o przychodzących wiadomościach (również wychodzących, w przypadku licencji ochrony poczty wychodzącej) oraz o zdarzeniach bezpieczeństwa, c) Raporty typu Top-N z zestawieniem określonych zdarzeń z określonego okresu.
WPE.8	System umożliwia filtrowanie poczty elektronicznej m.in. na podstawie: 1) Reputacji IP; 2) Reputacji Domeny; 3) Wieku Domeny; 4) Wyniku SPF, DKIM oraz DMARC; 5) Reputacji plików opartej o SHA; 6) Linków zawartych w treści lub temacie wiadomości (filtrowanie URL).
WPE.9	System zapewnia wsparcie mechanizmów SPF, DKIM oraz DMARC.
WPE.10	System zapewnia wsparcie dla S/MIME, TLS oraz DANE.
WPE.11	System wspiera przynajmniej jeden dodatkowy niezależny silnik antywirusowy firmy trzeciej bez konieczności wdrażania dodatkowych urządzeń.
WPE.12	System umożliwia analizę linków w treści, temacie oraz załącznikach wiadomości e-mail.
WPE.13	System wspiera analizę skróconych URL-i w celu wykrycia do jakiej witryny przekierowują.
WPE.14	System umożliwia tworzenie filtrów zawartości, by dostosować sposób filtrowania wiadomości e-mail.
WPE.15	System umożliwia wielokrotne wykorzystywanie w regułach predefiniowanych elementów takich jak filtry i akcje.
WPE.16	W ramach polityki system umożliwia definiowanie m.in. następujących akcji: 1) dostarczenie wiadomości z wykonaniem dodatkowych akcji: a) zmodyfikowanie tematu wiadomości, b) usunięcie i/lub dodanie nagłówka X-header, c) wysłanie kopii wiadomości pod wskazany adres lub adresy email, d) przepisanie (potencjalnie) niebezpiecznego linka oraz przekierowanie połączenia do chmurowego proxy producenta, które może ostrzec użytkownika przed zagrożeniem, bądź zablokować połączenie, e) zamianę linka na zdefiniowany przez administratora tekst, f) usunięcie załącznika wiadomości; 2) zablokowanie wiadomości; 3) przekierowanie wiadomości do wskazanej kolejki (kwarantanny); 4) wysłanie powiadomienia.
WPE.17	System udostępnia mechanizmy analizy i filtrowania oraz zarządzania treścią wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników.
WPE.18	System umożliwia filtrowanie i kontrolę treści w oparciu m.in. o: 1) słowa kluczowe;

Kod wymagania	Opis wymagań
	2) słowniki; 3) wyrażenia regularne; 4) typ załączników.
WPE.19	Kontrola obejmuje m.in. następujące elementy wiadomości: 1) tytuł; 2) treść; 3) nagłówki; 4) adres nadawcy; 5) adres odbiorcy.
WPE.20	System umożliwia zdefiniowanie polityki zarządzania treścią wiadomości w oparciu o wynik reputacji pobrany z bazy reputacji.
WPE.21	System umożliwia blokowanie plików na podstawie rozszerzenia, typu MIME oraz rzeczywistych artefaktów plików - tzw. „odcisków palca” (z ang. File-type fingerprinting).
WPE.22	System jest w stanie zidentyfikować kilkaset typów plików techniką file-type fingerprinting m.in.: 1) Archiwum: 7Z, ACE, ALZ, ARJ, BZ2, TBZ2, CAB, CPIO, DMG, EGG, EXE, GZ, ISO, JAR, LZH, OBD, RAR, RAR, RPM, SEA, EXE, SIT, SITX, TAR, ZIP; 2) Bazy danych: DB, DB3, DBF, IXA, IXB, IXC, MDB, ACCDB; 3) Wiadomości email i komunikatorów: DBX, EML, EMLX, EMLX, MBOX, MBX, MHT, MSG, OFT, OLK, PST, OST, VMBX, WINMAIL, DAT; 4) Multimedia: 3GP, AVI, FLAC, FLV, IFO, BUP, MID, MIDI, SMF, MOV, MP3, MP4, MPG, MSWMM, MXF, OGG, RM, SWF, VOB, WAV, AIFF, WMA; 5) Prezentacje: KEY, ODP, ODS, PPT, PPT, PPTX, SHOW, SXI, SDI, SDP; 6) Pliki graficzne: BMP, EPS, GFA, GIF, GIFF, ICO, JPEG, JPG, JPE, JIF, MDI, PCX, PNG, TIF, TIFF, WEBP; 7) Arkusze danych: CELL, CSV, FW3, NUMBERS, SXC, SXS, ODS, WK, WKS, WK3, WK4, WPS, XLS, XLSX, XLSB; 8) Pliki tekstowe i markup: CHM, HTM, HTML, ONE, ONETOC, RFT, TXT, DCA, RTF, SGML, TXT, XML; 9) Grafika wektorowa: AI, CDR, DGN, DWG, DXF, EMF, INDD, MCD, XMCD, PSD, VDX, VSDX, VSD, WMF, XPS, OXPS; 10) Dokumenty Office itp.: AMI, SAM, DOC, DOCX, DOX, FW3, GUL, HWP, IWP, JTD, JBW, JTT, LWP, M11, MANU, MNU, MAN, NDOC, NSF, ODT, PAGES, PDF, PS, PUB, PW, PW1, PW2, QA, QA3, QBB, QBW, QXx, QCxDW4, RFT, DCA, DW5, FFT, SXW, SDW, TTF, WPD, WP5, WRI, WS, WSx, WS2, WSD, XY; 11) Inne: BIN, CLASS, DCM, DLL, ELF, EXE, COM, SYS, HBX, HEX, HQX, LNK, LOG, MPP, MPX, MSI, ONE, TORRENT, UUE, VCF.
WPE.23	System umożliwia wykrywanie dokumentów używających skrypty (tzw. macro) i filtrowanie wiadomości na tej podstawie.
WPE.24	System umożliwia tzw. „rozbrajanie” niektórych typów plików (np. Word, PowerPoint) i prezentacje ich treści w formie bezpiecznego pliku PDF. System umożliwia także uprzednie skopiowanie oryginału wiadomości (i załącznika) oraz przesłania go do kwarantanny.
WPE.25	System umożliwia zdefiniowania polityki zarządzania treścią wiadomości w oparciu o wynik uwierzytelnienia DKIM.
WPE.26	System posiada mechanizm filtrowania treści za pomocą integracji z zewnętrznymi słownikami.
WPE.27	System umożliwia zarządzanie predefiniowanymi kolejkami (folderami) dla blokowanych wiadomości oraz tworzenia nowych.

Kod wymagania	Opis wymagań
WPE.28	System umożliwia budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu z zastosowaniem co najmniej: 1) domen email; 2) obiektów z Microsoft AD; 3) adresów pojedynczych użytkowników.
WPE.29	System zapewnia funkcjonalność ochrony przeciwko falom nowych ataków (z ang. Outbreak), działającą niezależnie od silników antywirusowych.
WPE.30	System umożliwia przekierowanie wiadomości e-mail do kwarantanny pozwalający na dalszą analizę administratorom i/lub użytkownikom końcowym.
WPE.31	Dla kolejki kwarantanny możliwe jest zdefiniowanie jej maksymalnej wielkości oraz czasu, po którym wiadomości będą usuwane.
WPE.32	System umożliwia przeniesie wiadomości do kwarantanny dostępnej dla użytkowników końcowych. Użytkownicy końcowi mają możliwość podglądu, usunięcia i uwolnienia wiadomości poddanych kwarantannie.
WPE.33	System posiada rozbudowane narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. W tym celu system zapewnia mechanizmy ochrony oparte m.in. na: 1) Sygnaturach; 2) Słownikach; 3) Heurystyce, dla której możliwa jest regulacja czułości (kontrola ilości False-Positives).
WPE.34	Mechanizm antyspamowy realizowany jest dwufazowo: 1) Pierwsza faza opiera się na sprawdzeniu reputacji adresu IP nadawcy w ogólnoświatowej bazie reputacji posiadającej następujące parametry: a) Otrzymuje dane z co najmniej 100.000 źródeł danych z całego świata. Analizuje ponad 150 parametrów dotyczących ruchu poczty elektronicznej i protokołu WWW (w tym co najmniej 90 dla poczty), b) Zwraca wynik reputacji dla adresu IP w skali 20-stopniowej - od -10 do 10, 2) System umożliwia wykorzystanie dwóch systemów badania reputacji nadawców dla poczty przychodzącej. Jeden z nich oparty jest o publiczny serwis Real-Time Blackhole List (RBL), drugi zaś jest systemem własnym producenta zaimplementowanym w rozwiązaniu; 3) Druga faza następuje, jeżeli wiadomość przejdzie pomyślnie fazę pierwszą. Opiera się silniku antyspamowym, korzystającym z reguł wysyłanych od producenta; 4) Reguły są tworzone dynamicznie na podstawie informacji z co najmniej trzech źródeł: a) ogólnoświatowej bazy danych reputacji o parametrach jak w fazie pierwszej, b) informacji zwrotnych od użytkowników rozwiązania, c) informacji od zespołu dedykowanych analityków bezpieczeństwa pracujących 24h na dobę, 7 dni w tygodniu, 365 dni w roku dla producenta rozwiązania; 5) Reguły weryfikują informacje na temat adresów IP pojawiających się w emailach jako linki do stron, strukturę wiadomości, sposób w jaki została wysłana, treść wiadomości oraz reputację nadawcy; 6) Reguły są uaktualniane automatycznie, przez Internet, nie rzadziej niż co 5 minut.
WPE.35	System umożliwia skorzystania z funkcji reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie weryfikacji oraz odrzucenie połączenia w przypadku: 1) Braku rekordu PTR w DNS; 2) niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS; 3) niezgodności rekordu reverse DNS (PTR) z rekordem forward DNS (A).

Kod wymagania	Opis wymagań
WPE.36	System umożliwia weryfikację nadawcy wiadomości w oparciu o mechanizm SPF (Sender Policy Framework) oraz podjęcie akcji, m.in.: 1) odrzucenie lub przyjęcie wiadomości, jeżeli rekord SPF nie istnieje; 2) odrzucenie wiadomości, jeżeli rekord SPF nie pasuje do domeny nadawcy.
WPE.37	System umożliwia monitorowanie i ograniczanie ilości jednoczesnych połączeń z jednego adresu IP, ograniczenie maksymalnej ilości wiadomości na jedno połączenie, ograniczenie maksymalnej ilości wiadomości na jednego odbiorcę oraz zdefiniowanie maksymalnego rozmiaru wiadomości.
WPE.38	Rozwiązanie pozwala na blokowanie przez określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów.
WPE.39	System posiada wbudowany webowy moduł zarządzający i raportujący.
WPE.40	Rozwiązanie jest wyposażone w system raportujący, umożliwiający m. in. 1) Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem (np. codziennie, co tydzień, co miesiąc); 2) Dostarczanie raportów w postaci plików pdf i csv; 3) Dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.
WPE.41	Istnieje możliwość zastosowania osobnego, scentralizowanego modułu raportowania tego samego producenta, który umożliwi obsługę logów z wielu urządzeń ochrony poczty elektronicznej na jednym systemie.
WPE.42	System umożliwia natywną integrację z chmurową platformą agregującą i korelującą telemetrię z innych rozwiązań bezpieczeństwa producenta (m.in. firewall, web proxy, EDR, sandbox, NDR, filtrowanie w warstwie DNS). Platforma ta zawarta jest w cenie subskrypcji systemu i nie wymaga dodatkowych licencji.
WPE.43	W celu ułatwienia pracy administratorów i analityków bezpieczeństwa, system daje możliwość płynnego przechodzenia między systemem ochrony poczty elektronicznej, a zintegrowaną chmurową konsolą agregującą telemetrię producenta (i vice versa), np. poprzez linki w interfejsie graficznym.
WPE.44	System wspiera zewnętrzne źródła informujące o zagrożeniach (z ang. threat feeds) z użyciem standarówd STIX/TAXII. Informacje otrzymane z użyciem STIX/TAXII mogą być użyte do filtrowania otrzymywanej poczty. Wspierane typy indykatorów kompromitacji (z ang. Indicators of Compromise) to m.in. adresy IP, skróty (hash-e) plików, domeny oraz pełne URL-e.
WPE.45	System może służyć jako sensor metadanych dla dodatkowej usługi antyphisingowej świadczonej z chmury producenta, która umożliwia analizę behawioralną poczty elektronicznej.
WPE.46	System daje możliwość manualnego wyszukiwania i remediacji (usunięcia) wiadomości już dostarczonych do skrzynki pocztowej użytkowników obsługiwanych przez Microsoft 365 lub lokalny serwer Microsoft Exchange.
WPE.47	System daje możliwość zaawansowanej ochrony antymalware sandbox.
WPE.48	Mechanizmy zaawansowanej ochrony antymalware obejmują m.in.: 1) Sprawdzenie reputacyjne dla min. 200 plików dziennie przesyłanych przez urządzenie; 2) Aktywną analizę przesyłanych plików przez mechanizm sandboxingu w chmurze publicznej bądź prywatnej; 3) Monitorowanie wsteczne dla plików już przesłanych.
WPE.49	Kontrola reputacji dla plików odbywa się z użyciem ogólnoświatowej bazy reputacji.

Kod wymagania	Opis wymagań
WPE.50	Kontrola reputacji odbywa się na podstawie unikalnych metadanych własnościowych pliku - sprawdzenie reputacyjne nie wymaga przesłania całego pliku na zewnątrz systemu kontroli poczty.
WPE.51	Funkcja wysyłania plików przesyłanych pocztą elektroniczną do analizy sandbox jest wbudowana w system ochrony poczty, bez konieczności stosowania zewnętrznych systemów firm trzecich.
WPE.52	Funkcja monitorowania wstecznego umożliwia informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez urządzenie. Dotyczy to sytuacji, gdy pliki przesyłane pocztą elektroniczną, po przejściu przez systemy ochrony antymalware i sandbox, są uznane za „dobre" lub „nieznane" i przesłane do odbiorcy. System przechowuje o tych plikach informacje (np. w postaci cache hash'y), by w przypadku zmiany dyspozycji (np. na skutek działania ekspertów bezpieczeństwa producenta, informacji zwrotnych od innych klientów itp.) administrator miał pełną świadomość, kto i kiedy takie pliki otrzymał, aby móc łatwo podjąć akcję remediacji.
WPE.53	Dla zagrożeń wykrytych dzięki monitoringowi wstecznemu, system daje możliwość automatycznej remediacji poprzez usunięcie wiadomości ze skrzynki pocztowej użytkowników obsługiwanych.
WPE.54	System posiada drugi komercyjny silnik antywirusowy z własną bazą sygnatur.

3. Wymagania dodatkowe.

Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia subskrypcji oraz wsparcia technicznego na opisane produkty, po wygaśnięciu zawartej umowy, bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla licencji, będących przedmiotem zamówienia.

4. Świadczenie serwisu gwarancyjnego i gwarancji.

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone oprogramowanie wykonawca zapewni serwis gwarancyjny liczony od daty podpisania protokołu odbioru produktu na okres 36 miesięcy opartego na świadczeniach serwisowych producenta.
WUS.02	Usługa wsparcia technicznego dla zakupionego produktu musi być realizowana w trybie 24 godzin na dobę, 7 dni w tygodniu, 365 dni w roku.
WUS.03	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu: 1) prawo do pobierania nowych wersji i aktualizacji; 2) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania; 3) dostęp do pomocy technicznej producenta; 4) nieograniczona ilość zgłoszeń serwisowych; 5) dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania/urządzeń; 6) dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji; 7) dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania; 8) dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania/urządzeń).
WUS.04	Do kontaktów/zgłoszeń Wykonawca udostępnia: 1) numer telefonu – _____ (infolinia bezpłatna), _____ (dla telefonów komórkowych i z zagranicy); 2) e-mail - _____. Do kontaktów/zgłoszeń Zamawiający udostępnia: 1) numer telefonu – _____; 2) e-mail - _____.
WUS.05	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
WUS.06	Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu, o którym mowa w wymaganiu WUS.04.
WUS.07	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
WUS.08	Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.

WUS.09	Dla oprogramowania obowiązują prawa gwarancyjne producenta.
WUS.10	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

5. Zasady odbioru przedmiotu zamówienia

I.Zasady Ogólne

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Księżycowej 5, w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35 lub w formie elektronicznej na wskazany przez Zamawiającego w Umowie adres e-mail.
3. Przedmiot Umowy podlegać będzie odbiorowi ilościowo - jakościowemu.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu ilościowo-jakościowego, którego wzór stanowi załącznik nr 3 do Umowy.

II.Odbiór ilościowo – jakościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności z ilością określoną w Umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.
3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach Umowy wraz z wymaganymi licencjami.
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego.