Opis Przedmiotu Zamówienia (OPZ)

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest zakup subskrypcji oprogramowania ochrony poczty elektronicznej w dopuszczalnych modelach: on-promises, hybrydowym, chmurowym (Inline+API lub MX-based) na które składa się:

1. 12000 subskrypcji oprogramowania.
2. wdrożenie funkcjonalności w środowisku IT Zamawiającego.
3. usługi wsparcia technicznego na okres 36 miesięcy.

II. Subskrypcje oprogramowania muszą zapewnić co najmniej niżej opisane wymagania:

Kategoria funkcjonalności	Funkcjonalność
Informacje ogólne	1. Oprogramowanie musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści itp.) 2. Oprogramowanie musi zapewnić ochronę przed atakami ukierunkowanymi. 3. Oprogramowanie musi zapewnić możliwość automatycznego wyciągania złośliwych wiadomości od użytkowników końcowych. 4. Oprogramowanie musi być dostarczone w postaci komplementarnego rozwiązania. 5. Oprogramowanie musi obsługiwać narzędzia lub interfejs programowania aplikacji (API) w celu integracji z innymi rozwiązaniami bezpieczeństwa w celu zapewnienia rozszerzonych funkcji. 6. Licencje muszą obejmować 12000 skrzynek pocztowych. 7. Oprogramowanie musi zapewniać funkcje wdrażania i zarządzania, natywnie (bezproblemowo) integrując się z oprogramowaniem Exchange (model hybrydowy) pakietu Microsoft Office w wersji 2016 i wyższej, zapewniając płynną i kompleksową integrację, w tym: • integrować się z platformą Microsoft 365 i przeprowadzać skan w poszukiwaniu złośliwych plików w obu usługach i wykrywać potencjalnie naruszenia kont w chmurze. • wykrywać i ostrzegać, które konto zostało naruszone, a następnie podejmować działania korygujące (blokować konto, resetować hasło). • zapewniać widoczność przejęcia konta: takich jak: potencjalnie narażone pliki, ryzyko dostępu OAuth, ryzyko związane z użytkownikiem i ryzyko udostępniania plików w pakietach i aplikacjach do współpracy w chmurze. 8. Oprogramowanie musi zapewnić symulacje ataków phishingowych 9. Zapewni odpowiednie subskrypcje na okres 36 miesięcy. 10. Oprogramowanie musi być dostosowane do wdrożenia w różnych środowiskach bezpieczeństwa IT i centrów operacji bezpieczeństwa (SOC), w tym lokalnych, hybrydowych i chmurowych. 11. Wykonawca zapewni na żądanie środowisko UAT (User Acceptance Testing), umożliwiające dokładne przetestowanie i walidację rozwiązania zabezpieczającego pocztę e-mail. 12. Wykonawca zapewni usługi generowania szczegółowych informacji poprzez wykorzystanie informacji o zagrożeniach pochodzących z rozwiązania zabezpieczającego pocztę e-mail, umożliwiając proaktywne wykrywanie, analizę i reagowanie na zagrożenia w oparciu o najnowsze informacje o zabezpieczeniach.

Dostępność	1. Oprogramowanie musi zapewnić zarządzanie za pomocą połączenia HTTPS przez przeglądarkę oraz poprzez protokół SSH. 2. Oprogramowanie musi zapewniać interfejs zarządzania z możliwością skutecznego śledzenia przepływu wiadomości e-mail, umożliwiając administratorom efektywne monitorowanie i analizowanie transakcji poczty e-mail. 3. Oprogramowanie musi w pełni obsługiwać Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) oraz Domain-based Message Authentication, Reporting & Conformance (DMARC) w celu uwierzytelniania domen e-mail, minimalizowania możliwości nadużywania domen i ochrony przed atakami typu domain spoofing na partnerów i klientów. 4. Oprogramowanie musi identyfikować ataki typu spoofing, displaying name spoofing i typo-squatting poprzez analizę nagłówka i treści wiadomości. 5. Oprogramowanie musi mieć możliwość automatycznego przekazywania wychodzącej wiadomości e-mail. (Rozwiązania innych firm korzystające z bram poczty e-mail do przekazywania wiadomości e-mail). 6. Oprogramowanie musi umożliwiać pracę w architekturze Master-Agent z możliwością przypisywania profili funkcjonalnych (filtrowania wiadomości, bazy kwarantanny, serwera logów) poszczególnym agentom. 7. Oprogramowanie musi pracować jako brama SMTP i być niezależnym od rodzaju stosowanego, chronionego serwera poczty. 8. Producent z odpowiednim wyprzedzeniem powiadomi o wszelkich patch'ach, uaktualnieniach, czy pracach konserwacyjnych. 9. Oprogramowanie musi zapewniać dostosowywalny portal zarządzania na podstawie uprawnień i wymagań użytkownika — kontrola dostępu oparta na rolach (RBAC). 10. Oprogramowanie musi zapewniać zdefiniowaną częstotliwość aktualizacji/poprawek (patches) w Platformie Bezpieczeństwa Poczty Elektronicznej (Miesięcznie / Kwartalnie / Rocznie). 11. Oprogramowanie musi obsługiwać synchronizację użytkowników i grup zarówno z lokalną usługą Active Directory (AD) za pośrednictwem protokołu push lub Lightweight Directory Access Protocol over SSL (LDAPS), jak i z usługą Azure AD. 12. Oprogramowanie musi realizować integrację z językiem Security Assertion Markup Language 2.0 (SAML 2.0) w celu płynnego uwierzytelniania i bezpiecznego dostępu. 13. Oprogramowanie musi zapewniać mechanizm uwierzytelniania jednokrotnego logowania (SSO) z usługą Active Directory lub zapewniać środki do synchronizacji haseł użytkowników. (Użytkownicy powinni mieć możliwość korzystania ze swojej standardowej nazwy użytkownika i hasła Active Directory w celu uzyskania dostępu do usługi) 14. W modelu chmurowym oprogramowanie musi zapewniać ograniczenia dostępu do portalu administracyjnego na podstawie określonych adresów IP Zamawiającego, zwiększając bezpieczeństwo poprzez ograniczenie dostępu tylko do autoryzowanych źródeł 15. Oprogramowanie musi zapewnić dedykowane statyczne publiczne adresy IP wyłącznie dla organizacji, zapewniając, że nie są one udostępniane innym organizacjom, zarówno do wysyłania, jak i odbierania wiadomości e-mail. 16. 14 Sprzedawca powinien być w stanie zaoferować na żądanie środowisko UAT (User Acceptance Testing), umożliwiające dokładne przetestowanie i walidację rozwiązania zabezpieczającego pocztę e-mail.

Kategoria funkcjonalności	Funkcjonalność
Filtrowanie poczty/Anty-spam/anty-virus	1. Oprogramowanie musi obsługiwać wymuszony protokół Transport Layer Security (TLS) 1.2 dla przychodzących i wychodzących wiadomości e-mail. 2. Oprogramowanie musi umożliwiać filtrowanie poczty przychodzącej dla wskazanych domen oraz przesyłanie ruchu pocztowego na wskazany serwer pocztowy. 3. Oprogramowanie musi bezproblemowo integrować się z lokalnymi bramkami pocztowymi za pośrednictwem przekazywania Mail Transfer Agent (MTA). 4. Oprogramowanie musi umożliwiać filtrowanie poczty wychodzącej do wskazanych przez Administratora serwerów pocztowych. 5. Oprogramowanie musi posiadać funkcjonalność przechowywania kopi wiadomości e-mail w pierwszym punkcie wejścia przez ograniczony czas, ułatwiając dochodzenie forensic poprzez zapewnienie wiarygodnego i dostępnego źródła danych e-mail do analizy Business Email Compromise (BEC), AI / ML, behavioral & reputation. 6. Oprogramowanie musi zapewnić możliwość zdefiniowania osobnych tras przesyłania poczty dla ruchu przychodzącego i wychodzącego w oparciu o statyczne wpisy adresów serwerów, smart hosta lub rekordy MX serwerów DNS. 7. Oprogramowanie musi zapewniać skutecznie blokowanie różnych ataków opartych na wiadomościach e-mail, w tym Business Email Compromise (BEC), złośliwe oprogramowanie malware, phishing i włamanie do konta e-mail (EAC). 8. Oprogramowanie musi wykorzystywać technologię antyphishingową, która wykorzystuje AI/ML do wykrywania wzorców komunikacji i anomalii w stylu konwersacji, a także weryfikacji podejrzanych adresów URL, zapewniając ukierunkowaną ochronę przed atakami BEC. 9. Oprogramowanie musi być w stanie dynamicznie analizować zarówno zawartość nagłówka, jak i wiadomości w celu wykrywania i identyfikowania ataków polegających na podszywaniu się pod domenę, podszywaniu się pod wyświetlaną nazwę (lookalike domain attack). 10. Oprogramowanie musi zapewniać funkcjonalność klasyfikacji, który wykorzystuje usługę oceny spamu złożonego i uczenie maszynowe w celu poznania wzorców ruchu e-mail organizacji i proaktywnej ochrony przed atakami BEC. 11. Oprogramowanie musi umożliwiać analizę łańcucha kontaktów opartego na AI/ML w celu identyfikacji i obrony przed atakami socjotechnicznymi, podszywającymi się pod inne osoby lub BEC. 12. Oprogramowanie musi obsługiwać sandbox na wielu platformach, wiodących vendorów, np. Azure, Google, itp. 13. Oprogramowanie musi posiadać lokalną kwarantannę dla zainfekowanych wiadomości. 14. Oprogramowanie musi zapewniać użytkownikom końcowym możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny. 15. Oprogramowanie musi umożliwiać określanie poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników. 16. Kwarantanna użytkownika oraz skrócone informacje o stanie kwarantanny dla użytkownika muszą być dostępne w języku polskim. 17. Oprogramowanie musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych. 18. Oprogramowanie musi umożliwiać zmianę wyglądu portalu kwarantanny

	dla użytkownika końcowego, zarówno co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów. 19. Oprogramowanie musi umożliwiać definiowanie i przeglądanie wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych. 20. Dla wszystkich stworzonych folderów kwarantanny oprogramowanie musi zapewniać możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie. 21. Oprogramowanie musi umożliwiać wyszukiwanie wiadomości w kwarantannie na podstawie nadawcy, odbiorcy, tematu wiadomości lub czasu od kiedy wiadomość znajduje się w kwarantannie. 22. Oprogramowanie musi umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do innego odbiorcy, przeniesienie do innego folderu, zwolnienie wiadomości, zwolnienie zaszyfrowanej wiadomości, ponowną ocenę wiadomości przez moduły filtrujące. 23. Oprogramowanie musi zapewnić możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta oprogramowania na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego. 24. Oprogramowanie musi zapewniać kompleksową ochronę przed atakami phishingowymi, w tym zaawansowaną ochronę przed phishingiem, wykrywanie oszustów i wewnętrzną ochronę poczty e-mail. 25. Oprogramowanie musi proaktywnie działać w oparciu o sandboxing i analizować podejrzane adresy URL za pomocą analizy dynamicznej/behawioralnej, aby zapobiec rozprzestrzenianiu się złośliwego oprogramowania i innych zagrożeń 26. Oprogramowanie musi być w stanie blokować złośliwe adresy URL i wykorzystywać przepisywanie adresów URL, a także zapewniać konfigurowalne strony blokowania dla niebezpiecznych witryn, aby edukować użytkowników o potencjalnych zagrożeniach. 27. Oprogramowanie musi wykorzystywać technologie AI/ML w celu zwiększenia wykrywania zagrożeń związanych z pocztą e-mail. 28. Oprogramowanie musi wykorzystywać sztuczną inteligencję/uczenie maszynowe do analizowania wzorców komunikacji, aby zapobiegać przychodzącym wyłudzaniu informacji i wykrywać potencjalnie błędnie skierowane wiadomości e-mail 29. Oprogramowanie musi obsługiwać tworzenie niestandardowych reguł wyłudzania informacji i analizę AI/ML w celu wykrywania ukierunkowanych ataków phishingowych o mniejszej ilości. 30. Oprogramowanie musi zapewniać integrację API z platformami współpracy w celu filtrowania złośliwych treści lub podejrzanych interakcji, zapewniając kompleksowe podejście do bezpieczeństwa poczty e-mail. 31. Oprogramowanie musi zapewniać ochronę przed atakami DoS i Directory Harvest. 32. Oprogramowanie musi zapewniać ochronę przed atakami polegającymi na zbieraniu danych uwierzytelniających (wiadomość phishingowa, która zachęca ofiarę do kliknięcia hiperłącza prowadzącego do fałszywej strony logowania). 33. Oprogramowanie musi zapewniać ochronę przed spear-phishingiem, oraz opóźnionymi exploitami. 34. Oprogramowanie musi zapewniać analizy z wykorzystaniem technik anti-evasion techniques.

	35. Oprogramowanie musi obsługiwać nadpisywanie adresów URL zarówno dla przychodzących, jak i wychodzących wiadomości e-mail, w celu zapewnienia bezpiecznego wykonywania izolacji. 36. Oprogramowanie musi przeprowadzać inspekcję adresów URL w czasie rzeczywistym w treści wiadomości e-mail, załącznikach (PDF, dokumentach pakietu Office) oraz witrynach udostępniania plików (OneDrive, SharePoint). 37. Oprogramowanie musi być w stanie wykorzystać analizę obrazów AI/ML do wykrywania złośliwych adresów URL i ich blokowania. 38. Oprogramowanie musi blokować adresy URL na podstawie reputacji adresów URL przed dostarczeniem przy użyciu analizy predykcyjnej (predictive intelligence). 39. Oprogramowanie musi obsługiwać ochronę adresów URL po dostarczeniu, np. analizę zawartości adresów URL w sandboxie 40. Rozwiązanie musi stale sprawdzać i analizować złośliwe adresy URL po dostarczeniu (wstecznie) i umożliwiać administratorom czyszczenie/usuwanie wiadomości e-mail, których dotyczy problem, (monitorowanie zachowania adresu URL pod kątem opóźnionych ataków wykorzystujących luki) 41. Rozwiązanie musi być w stanie zaoferować weryfikację adresów internetowych (URL) w wiadomościach e-mail na podstawie czasu kliknięcia 42. Rozwiązanie musi zapewniać izolowane i tylko do odczytu środowiska kontenerów do wykonywania podejrzanych adresów URL i linków w wiadomościach e-mail (wiadomości lub załącznikach) 43. Rozwiązanie musi być w stanie zdekodować przepisane adresy URL w celu zidentyfikowania oryginalnej witryny docelowej 44. Rozwiązanie musi być w stanie utrzymać dostarczanie wiadomości e-mail, podczas gdy wszystkie adresy URL i linki w wiadomości e-mail są analizowane 45. Rozwiązanie musi umożliwiać administratorom zastępowanie blokad adresów URL i podejmowanie świadomych decyzji o zezwoleniu 46. Rozwiązanie musi być w stanie izolować strony internetowe i wymuszać tryb tylko do odczytu, aby zapobiec nieautoryzowanemu przesyłaniu danych uwierzytelniających i danych użytkownika. 47. Rozwiązanie nie powinno przechowywać danych wiadomości e-mail i załączników w magazynie statycznym na platformie izolacji. 48. Oprogramowanie musi obsługiwać dokładne wykrywanie i blokowanie złośliwych wiadomości e-mail wykorzystujących automatyczną analizę złośliwego oprogramowania, w tym: • blokowanie wiadomości e-mail od znanych podejrzanych nadawców; • skanowanie załączników za pomocą programu antywirusowego; • blokowanie wiadomości e-mail ze znanymi nieprawidłowymi adresami URL; • analiza treści w celu identyfikacji spamu. 49. Oprogramowanie musi zapewniać zaawansowane funkcjonalności ochrony, w tym: • przepisywanie adresów URL; • skanowanie w wielu programach antywirusowych (AV); • integracja z rozwiązaniami SandBox (np.Trelix); • kwarantanna spamu; • obsługę Graymail; • ochrona biznesowej poczty tzw. BEC.

	• Usuniecie wiadomości po dostarczeniu. . 50. Oprogramowanie musi zapewniać wysoką dostępność usług, aby sprostać potrzebom biznesu. 51. Oprogramowanie musi zapewniać pełną ochronę przed znanymi zagrożeniami ze strony złośliwego oprogramowania. 52. Oprogramowanie musi charakteryzować się niskim wskaźnikiem wyników fałszywie dodatnich, a jednocześnie skutecznie identyfikować i blokować złośliwą zawartość. 53. Oprogramowanie musi obsługiwać niskie opóźnienia poczty e-mail. 54. Oprogramowanie musi zapewniać skutecznie skanować i zwalniać załączniki w odpowiednim czasie. 55. Oprogramowanie zapewni obsługę klasyfikacji wiadomości, w tym oddzielne klasyfikatory dla spamu, podszywania się, wiadomości zbiorczych, wyłudzania informacji, wiadomości dla dorosłych i złośliwego oprogramowania, z możliwością modyfikacji progów punktacji dla każdej kategorii. 56. Oprogramowanie musi obsługiwać skanowanie i stosowanie określonych reguł dla zaszyfrowanych lub chronionych hasłem i wielokrotnie skompresowanych plików. 57. Oprogramowanie musi obsługiwać automatyczne wykrywanie nowych kampanii spamowych . 58. Oprogramowanie musi być w stanie automatycznie usuwać podejrzane wiadomości e-mail ze skrzynek odbiorczych użytkowników 59. Oprogramowanie musi zapewniać szczegółowe mechanizmy kontroli administracyjnej (RBAC), aby umożliwić dostęp oparty na rolach do każdego modułu i folderu kwarantanny. 60. Oprogramowanie musi zezwalać użytkownikowi końcowemu na dostęp do wiadomości innych niż złośliwe poddane kwarantannie, jednocześnie uniemożliwiając dostęp do złośliwych wiadomości. 61. Oprogramowanie musi spełniać skomplikowane wymagania dotyczące routingu poczty, w tym routingu grupowego opartego na grupach użytkowników. 62. Oprogramowanie musi korzystać z zaawansowanych technik ochrony przed kradzieżą poświadczeń i analizy przetwarzania obrazów w celu wykrywania i blokowania ataków wyłudzających informacje, które podszywają się pod strony logowania. 63. Oprogramowanie musi wykorzystywać uczenie maszynowe do ciągłego monitorowania i dostosowywania się do wzorców komunikacji e-mail w organizacji, zapewniając lepsze wykrywanie zagrożeń i reagowanie na nie. 64. Oprogramowanie musi zapewniać skuteczne możliwości wykrywania spamu w wielu językach. 65. Oprogramowanie musi umożliwiać administratorom przypisywanie różnych zestawów reguł na podstawie określonych adresów e-mail w celu poprawy zarządzania pocztą e-mail i bezpieczeństwa. 66. Oprogramowanie musi oferować weryfikację odbiorcy w usłudze Active Directory i innych źródłach list e-mail, aby zapobiec spoofingowi wiadomości e-mail i usprawnić dostarczanie wiadomości e-mail 67. Oprogramowanie musi obsługiwać szereg zachowań i akcji routingu dla różnych scenariuszy, umożliwiając administratorom dostosowanie obsługi poczty e-mail w oparciu o określone potrzeby i wymagania. 68. Oprogramowanie musi obsługiwać wychodzące lub przychodzące wiadomości e-mail, w tym zarządzanie stopką (stopki prawnej lub stopki

	zgodności) : • filtrowanie na podstawie atrybutów poczty e-mail lub atrybutów Active Directory, • na podstawie polityki / atrybutu lub nie stosuj, jeśli wiadomość e-mail jest zaszyfrowana za pomocą S/MIME lub podpisana cyfrowo itp.; • stosowanie podpisów i zastrzeżeń na podstawie grup użytkowników AD. 69. Oprogramowanie musi obsługiwać możliwość zarządzania stopkami w przychodzących i wychodzących wiadomościach e-mail, w tym stopkami prawnymi i zgodności, z możliwością stosowania różnych filtrów na podstawie atrybutów poczty e-mail lub usługi Active Directory. Musi również obsługiwać wielojęzyczne i dynamiczne wstawianie zawartości oraz selektywnie stosować stopki na podstawie zasad, atrybutów lub stanu szyfrowania. Ponadto rozwiązanie musi zapewniać możliwość stosowania podpisów i zastrzeżeń na podstawie grup użytkowników usługi AD. 70. Oprogramowanie musi umożliwiać użytkownikom końcowym otrzymywanie niestandardowych powiadomień e-mail na podstawie nazwy domeny. 71. Oprogramowanie musi obsługiwać uwierzytelnianie dwuskładnikowe dla użytkowników końcowych, administratorów platformy i administratorów systemu. 72. Oprogramowanie w modelu chmurowym musi zapewniać internetową konsolę zarządzania i konfiguracji, która centralizuje konfigurację, rejestrowanie, kwarantannę i raportowanie systemu, która jest kompatybilna z nowoczesnymi przeglądarkami w zakresie konfiguracji i zarządzania. 73. Oprogramowanie musi obsługiwać kontrolę dostępu opartą na rolach do konsoli zarządzania, w której nazwanym kontom administratorów można przypisać określone uprawnienia w interfejsie zarządzania (RBAC). 74. Oprogramowanie musi zapewniać administratorom możliwości zarządzania kolejką poczty e-mail. 75. Oprogramowanie musi umożliwiać delegowanie administracji do podorganizacji w oparciu o logiczne grupowania użytkowników, takie jak jednostki biznesowe, regiony geograficzne, role, funkcje lub hierarchia organizacyjna. Organizacje podrzędne muszą mieć możliwość dziedziczenia zasad z organizacji głównej, ale muszą mieć również możliwość zastępowania zasad z unikatowymi atrybutami specyficznymi dla tej organizacji podrzędnej. 76. Oprogramowanie musi obsługiwać powiadamianie zespołu ds. zabezpieczeń (SOC) o wszystkich zasadach, folderach kwarantanny i progach kolejki. 77. Oprogramowanie musi być w stanie ograniczyć rozmiar wiadomości e-mail, które mogą być wysyłane/odbierane, lub liczbę adresatów objętych dostarczaniem. 78. Oprogramowanie musi zapewniać natywne narzędzia do rozwiązywania problemów z routingiem aplikacji i wiadomości z możliwością śledzenia wiadomości. 79. Oprogramowanie musi obsługiwać tworzenie list bezpiecznych/zablokowanych na podstawie użytkowników lub grup użytkowników. 80. Oprogramowanie musi zapewniać automatyzację przy importowaniu użytkowników/grup z list bezpiecznych/zablokowanych przy użyciu min. plików CSV/tekstowych.

	81. Oprogramowanie musi być w stanie obsługiwać i filtrować biuletyny informacyjne i masowy spam e-mail. 82. Oprogramowanie musi zapewnić wykrywanie ataków spamowych opartych na tekście, obrazach, multimediach i załącznikach. 83. Oprogramowanie muszą obsługiwać ukierunkowane blokowanie wiadomości e-mail ze spamem. 84. Oprogramowanie musi być w stanie wykryć kampanie spamowe i dodać źródło kampanii do czarnej listy, natychmiast blokując połączenia z tego serwera pocztowego. 85. Oprogramowanie musi zapewniać ochronę przed nękaniem poczty i ograniczać ryzyko związane z wiadomościami e-mail od nieznanych nadawców, szczególnie dla kadry kierowniczej lub VIP-ów, chroniąc ich przed potencjalnymi zagrożeniami i zapewniając bezpieczeństwo komunikacji e-mail. 86. Oprogramowanie musi obsługiwać filtrowanie połączeń w oparciu o reputację zagrożeń, co pozwala na identyfikację i filtrowanie wiadomości e-mail na podstawie domen lub adresów IP, z których są wysyłane, zwiększając zdolność do łagodzenia potencjalnych zagrożeń 87. Oprogramowanie musi być w stanie zintegrować się z silnikami antywirusowymi i antymalware innych firm w celu filtrowania wiadomości e-mail. 88. Oprogramowanie musi zapewniać blokowanie niektóre typy plików na podstawie rozszerzeń, takich jak .exe, .dll, .doc/.docx, .xls/.xlsx, .ppt/.pptx, .jpg, .png, .pdf, .swf, .mp3/.mp4, .java, .vbs itp. 89. Oprogramowanie musi być w stanie blokować archiwa załączników, takie jak .zip, .tgz, .7zip, .cab, .lzh, .rar, .tnef itp
Raportowanie	1. Oprogramowanie musi zapewniać widoczność zagrożeń bezpieczeństwa w organizacji, w tym • najczęściej atakowane konta e-mail; • w jaki sposób te konta są atakowane; • użytkownicy o zachowaniach wysokiego ryzyka; • w jaki sposób ci ryzykowni użytkownicy uzyskują dostęp do danych. 2. Oprogramowanie musi dostarczyć złożone Raporty i filtrować dane zawierające liczbę wiadomości E-mail na podstawie: • filtry czasu; • spam, masowe wiadomości e-mail, wyłudzanie informacji; • złośliwe wiadomości e-mail (antywirusowe, anty-malware, piaskownica); • najczęściej błędne adresy URL; • złe domeny; • ataki ukierunkowane z wybranego obszaru geograficznego. 3. Rozwiązanie musi zapewniać szczegółowe, bogate w kontekst i umożliwiające podejmowanie działań analizę zagrożeń, w tym wskaźnik naruszenia bezpieczeństwa (IOC) i informacje o odbiorcach. 4. Oprogramowanie musi posiadać funkcjonalność predefiniowanych szczegółowych raportów obejmujących użycie oprogramowania i inne obszary, w tym globalne podsumowanie wiadomości, spam, wirusy i inne działania reguł, aby zaoszczędzić czas i wysiłek administratora związany z gromadzeniem danych do raportów o stanie 5. Raporty powinny mieć możliwość przesłania przez e-mail, lub pobierać w formacie CSV. 6. Oprogramowanie musi mieć zapewniać wyświetlanie przez administratorów raportów zawierających szczegółowe statystyki dotyczące przetworzonych wiadomości e-mail, odrzuconych wiadomości e-mail, transakcji SMTP i przepływów komunikacji. 7. Oprogramowanie zapewni możliwość porównania i dotkliwość ataków na inne organizacje z branży lub grupy porównawcze. 8. Oprogramowanie informacje o tym, kto atakuje organizację (TI). 9. Oprogramowanie będzie umożliwiało zdolność do zrozumienia, czy

	wiadomości są częścią ukierunkowanej kampanii skierowanej do organizacji. 10. Oprogramowanie zapewni zaawansowane pulpity administracyjne obrazujące zagrożenia, trendy i analizy złośliwego oprogramowania i spamu, analizę sadnbox, kliknięcia adresów URL. 11. Oprogramowanie musi zawierać możliwość predefiniowanych raportów o zamiarach atakujących (np. złośliwe oprogramowanie, kradzież danych uwierzytelniających, podszywanie się itp.) oraz próbach oprogramowania wymuszającego okup (. 12. Rozwiązanie musi zapewniać szczegółowe raportowanie w oparciu o liczbę i typy wiadomości e-mail zgłaszanych przez użytkowników oraz rozumieć trendy ataków wpływające na organizację. 13. Rozwiązanie musi zapewniać szczegółowe informacje oparte na ryzyku i zalecać kontrolę zabezpieczeń na podstawie szczegółowych informacji. 14. Rozwiązanie musi zapewniać eksport danych do interfejsu API w celu integracji z rozwiązaniami klasy SIEM/SOAR.