|  |  |
| --- | --- |
| **Ministerstwo Rozwoju i Technologii**  **ul. Plac Trzech Krzyży 3/5**  **00-507 Warszawa** | **Warszawa, 25.11.2022 r.** |

**ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA**

Ministerstwo planuje uruchomić postępowanie przetargowe na zakup subskrypcji oprogramowania do ochrony poczty elektronicznej.

## Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego na zakup subskrypcji oprogramowania do ochrony poczty elektronicznej.

1. **PRZEDMIOT ZAMÓWIENIA**

Przedmiotem Zamówienia jest zakup subskrypcji oprogramowania do ochrony poczty elektronicznej na które składa się:

1. 1500 subskrypcji oprogramowania Proofpoint - PFPT Email Protection F-Secure;
2. 1500 subskrypcji oprogramowania Proofpoint - PFPT Threat Response Auto-Pull-V-mSOAR
3. 1500 subskrypcji Proofpoint PFPT TAP URL & Attachment Bundle;
4. usługi wsparcia technicznego Proofpoint - PFPT Platinum Level Support na okres 12 miesięcy
5. **TERMIN REALIZACJI ZAMÓWIENIA**

Przedmiot zamówienia zostanie zrealizowany w terminie **do 10 dni** od daty zawarcia umowy

1. **MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem Zamówienia jest zakup subskrypcji oprogramowania do ochrony poczty elektronicznej **lub równoważnego spełniającego wymagania określone w niniejszym rozdziale.**

**Równoważne licencje oprogramowania** **muszą spełniać 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 zamkniętego rozwiązania sprzętowego lub obrazu maszyny wirtualnej. 5. Licencje muszą obejmować 1500 skrzynek pocztowych. 6. Należy zapewnić odpowiednie licencje na okres 12 miesięcy. |
| Dostępność | 1. Oprogramowanie musi zapewnić lokalne i zdalne zarządzanie za pomocą połączenia HTTPS przez przeglądarkę oraz poprzez protokół SSH. 2. Oprogramowanie musi umożliwiać pracę w architekturze Master-Agent z możliwością przypisywania profili funkcjonalnych (filtrowania wiadomości, bazy kwarantanny, serwera logów) poszczególnym agentom. 3. Oprogramowanie musi pracować jako brama SMTP i być niezależnym od rodzaju stosowanego, chronionego serwera poczty. |
| Filtrowanie poczty | 1. Oprogramowanie musi umożliwiać filtrowanie poczty przychodzącej dla wskazanych domen oraz przesyłanie ruchu pocztowego na wskazany serwer pocztowy. 2. Oprogramowanie musi umożliwiać filtrowanie poczty wychodzącej do wskazanych przez Administratora serwerów pocztowych. 3. 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. 4. Oprogramowanie w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących: AV, antyspam, kontrola treści. 5. Oprogramowanie musi umożliwiać automatyczne pobieranie oraz instalowanie aktualizacji modułów ochronnych oraz całego oprogramowania 6. Oprogramowanie musi posiadać lokalną kwarantannę dla zainfekowanych wiadomości. 7. Oprogramowanie musi zapewniać użytkownikom końcowym możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny. 8. Oprogramowanie musi umożliwiać określanie poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników. 9. Kwarantanna użytkownika oraz skrócone informacje o stanie kwarantanny dla użytkownika muszą być dostępne w języku polskim. 10. Oprogramowanie musi zapewniać możliwość uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny. W tym celu, oprogramowanie musi wspierać mechanizmy uwierzytelnienia jednokrotnego (Single Sign-On) oparte o usługi federacyjne domeny Active Directory (ADFS) lub protokół SAML 2.0. 11. Oprogramowanie musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych. 12. 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. 13. Oprogramowanie musi umożliwiać definiowanie i przeglądanie wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych. 14. Dla wszystkich stworzonych folderów kwarantanny oprogramowanie musi zapewniać możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie. 15. Oprogramowanie musi umożliwiać wyszukiwanie wiadomości w kwarantannie na podstawie nadawcy, odbiorcy, tematu wiadomości lub czasu od kiedy wiadomość znajduje się w kwarantannie. 16. 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. 17. Oprogramowanie musi zapewnić możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta oprogramowania na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego. 18. Oprogramowanie musi umożliwiać stworzenie bazy użytkowników poczty elektronicznej w oparciu o zdefiniowanie lokalnych kont użytkowników, a także zapewniać możliwość synchronizacji bazy użytkowników z serwerów: Active Directory, Azure Active Directory, LDAP, MS Exchange, Lotus Domino lub za pomocą odpowiednio przygotowanych plików (tekstowych, csv). 19. Oprogramowanie musi zapewniać możliwość ustawienia przez administratora harmonogramu synchronizacji bazy użytkowników. 20. Oprogramowanie musi umożliwiać konfigurację harmonogramu wysyłania powiadomień mailowych do użytkowników o np. nowych wiadomościach zatrzymanych w kwarantannie. 21. Oprogramowanie musi posiadać graficzny interfejs administratora do śledzenia wiadomości na poziomie modułu MTA i modułach filtrujących na podstawie parametrów: odbiorca, nadawca, nazwa załącznika, temat wiadomości, sender hostname lub IP, nazwa reguły filtrującej, Message ID, nazwa wirusa, numer sesji. 22. Oprogramowanie musi zapewniać możliwość tworzenia własnych reguł filtrowania treści w oparciu o: adresy IP nadawców odbiorców, adresy email, typ i rozmiar załącznika, ilość załączników, treść maila, pola nagłówka wiadomości, treść załączników. 23. Oprogramowanie musi umożliwiać tworzenie własnych reguł filtrowania lub klonowania istniejących. 24. Oprogramowanie musi umożliwiać tworzenie słowników słów kluczowych. 25. Oprogramowanie musi zapewniać mechanizm weryfikacji poprawności nazwy odbiorcy na podstawie zapytań wysyłanych do serwera LDAP, SMTP lub lokalnego repozytorium użytkowników. 26. Oprogramowanie musi zapewniać wsparcie dla standardu Sender Policy Framework (SPF). 27. Oprogramowanie musi zapewniać wsparcie dla standardu Domain Keys Identified Mail (DKIM). 28. Oprogramowanie musi zapewniać wsparcie dla standardu Domain-based Message Authentication Reporting & Conformance (DMARC). 29. Ochrona antywirusowa musi być realizowana poprzez silniki zasilane w sygnatury oraz filtr analizy heurystycznej wykrywający ataki typu zero hour. 30. Oprogramowanie musi umożliwiać przegląd ostatnich infekcji oraz listę najczęstszych zagrożeń. 31. Aktualizacje sygnatur modułu antywirusowego muszą być dostępne nie rzadziej niż raz na dobę. 32. Oprogramowanie musi zapewniać możliwość tworzenia wielu polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości. 33. Oprogramowanie musi zapewniać możliwość definiowania różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa. 34. Oprogramowanie musi zapewniać możliwość określenia zasad postępowania z zabezpieczonymi wiadomościami (zawierającymi załączniki chronione hasłem, podpisanymi kluczem kryptograficznym lub zabezpieczonymi S/MIME, DKIM). 35. Moduł detekcji spamu musi bazować na metodzie zaawansowanej analizy heurystycznej, która wyklucza konieczność ręcznego tworzenia reguł w razie pojawienia się nowych technik omijania filtrów antyspamowych. 36. Oprogramowanie musi umożliwiać korzystanie ze źródeł producenta, niepublicznych serwerów badania reputacji nadawców maila. 37. Oprogramowanie musi zapewniać możliwość automatycznej oceny reputacji źródła przesyłanego maila (na podstawie weryfikacji ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości sklasyfikowanych jako spam) z możliwością limitowania ilości odbieranych wiadomości w określonej jednostce czasu od źródeł o niskiej reputacji. 38. Oprogramowanie musi zapewniać możliwość definiowania reguł antyspamowych na poziomie całego środowiska, grup użytkowników oraz pojedynczych użytkowników. 39. Oprogramowanie musi zapewniać możliwość tworzenia systemowych list bezpiecznych i zablokowanych nadawców, odbiorców, hostów, domen lub adresów IP. 40. Oprogramowanie musi zapewniać inteligentne rozpoznawanie typów analizowanych załączników. Zmiana rozszerzeń powinna być ignorowana przez oprogramowanie i nie powinna być metodą omijania tego typu filtra. 41. Oprogramowanie musi zapewniać ochronę przeciwko atakom typu Odmowa dostępu do usługi (Denial Of Service) oraz wykrywać i blokować próby enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack). 42. Oprogramowanie musi posiadać mechanizm ochrony przed zjawiskiem wykorzystania wiadomości niedostarczonych (Fake NDR – Non-Delivery Receipt) za pomocą cyfrowego oznaczenia wiadomości wysyłanych z chronionych domen organizacji). 43. Oprogramowanie musi zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security. |
| Ochrona przed atakami ukierunkowanymi | 1. Oprogramowanie musi zapewniać mechanizmy ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi, które wykorzystują załączniki lub hiperłącza (adresy URL) w celu zainstalowania na urządzeniu użytkownika szkodliwego oprogramowania lub skłonienia użytkownika do ujawniania haseł lub innych poufnych danych. 2. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi stanowić integralną część oprogramowania i nie może wymagać zastosowania dodatkowej maszyny wirtualnej lub urządzenia fizycznego. 3. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi zapewniać przynajmniej mechanizmy ochrony przed:    1. Niebezpiecznymi załącznikami.    2. Niebezpiecznymi hiperłączami (adresami URL prowadzącymi do niebezpiecznych stron WWW typu phishing lub malware). 4. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi umożliwiać zatrzymanie analizowanej wiadomości w systemowej kolejce do momentu otrzymania werdyktu o zagrożeniu w analizowanym załączniku lub łączu URL wiadomości. 5. Oprogramowanie musi zapewniać możliwość wyboru trybu analizy załączników przez moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi przynajmniej w zakresie:    1. sprawdzenia wyłącznie reputacji pliku poprzez porównaniu jego skrótu z bazą skrótów znanych zagrożeń.    2. wieloetapowej analizy dynamicznej, obejmującej uruchomienie pliku w izolowanym środowisku typu sandbox. 6. Środowisko analizy dynamicznej typu sandbox powinno być elementem modułu ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi. 7. W celu zapewnienia wysokiej dostępności, wydajności i skalowalności środowisko analizy dynamicznej typu sandbox musi pochodzić od tego samego producenta co oferowane oprogramowanie ochrony poczty elektronicznej i być dostarczane w modelu oprogramowanie jako usługa (SaaS). 8. Zbiór analizowanych typów plików przez moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi powinien obejmować przynajmniej:    1. MS Office (Word, Excel, Power Point).    2. PDF.    3. Adobe Flash.    4. HTML, TXT,RTF.    5. EML.    6. Pliki skompresowane (ZIP, TAR, RAR, GZIP, 7ZIP). 9. W przypadku analizy plików zabezpieczonych hasłem (zaszyfrowanych), oprogramowanie musi podjąć próbę odszyfrowania tych plików wykorzystując słowa lub ciągi słów, wybrane metodą heurystyczną, z treści analizowanej wiadomości. 10. Oprogramowanie musi umożliwiać określenie maksymalnego dopuszczalnego czasu analizy załączników przez moduł ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi oraz wybór odpowiedniej dyspozycji na wiadomości (prześlij dalej / zablokuj / zatrzymaj w kwarantannie) w przypadku przekroczenia tego czasu. 11. Moduł ochrony przed niebezpiecznymi hiperłączami (adresami URL prowadzącymi do stron typu phishing lub malware) musi wykorzystywać mechanizmy analizy predykcyjnej w celu identyfikacji podejrzanych hiperłączy i wiadomości, zanim wiadomości zostaną dostarczone na skrzynki odbiorcze użytkowników. Proces wyszukiwania podejrzanych hiperłączy oraz analiza dynamiczna stron internetowych, do których te łącza prowadzą, musi być realizowany przez producenta oprogramowania na zbiorze przynajmniej 50 milionów unikalnych adresów URL na minutę i być niezależny od wiadomości dostarczanych do organizacji Zamawiającego. 12. Ochrona przed niebezpiecznymi hiperłączami powinna polegać na przepisywaniu adresów URL, zawartych w treści wiadomości lub w jej załącznikach do formatu umożliwiającego śledzenie kliknięć użytkowników i zablokowania prób wejścia użytkowników na niebezpieczne strony WWW. 13. Po kliknięciu przez użytkownika w hiperłącze poddane analizie predykcyjnej, w oknie przeglądarki internetowej użytkownika powinien zostać wyświetlony:     1. Komunikat o wykrytym zagrożeniu i zablokowaniu wejścia na żądaną stronę.     2. oryginalna strona WWW – jeśli w wyniku przeprowadzonej analizy nie znaleziono zagrożenia. 14. W przypadku kliknięcia przez użytkownika w hiperłącze nieobjęte analizą predykcyjną, w oknie przeglądarki internetowej użytkownika musi zostać wyświetlona oryginalna strona WWW, a oprogramowanie musi rozpocząć analizę tej strony w środowisku sandbox. Proces analizy dynamicznej musi być transparentny dla użytkownika. W przypadku wykrycia zagrożenia, oprogramowanie musi wygenerować alarm o odpowiednim poziomie krytyczności (Major lub Critical), wysłać mailowe powiadomienie do administratorów o zaistniałym zdarzeniu oraz przekazać w sposób automatyczny alarm, wraz z informacjami o zaistniałym zdarzeniu, do systemu klasy SOAR, który podejmie w sposób automatyczny odpowiednie reakcje naprawcze. 15. Wraz z modułem ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi, producent oprogramowania musi zapewnić dostęp do portalu WWW prezentującego informacje o wykrytych zagrożeniach, w zakresie min.: wektor ataku (załącznik / hiperłącze), źródło i cel ataku, atrybuty wiadomości będącej nośnikiem ataku, wykorzystana technika ataku, poziom krytyczności wykrytego zagrożenia, globalny zasięg ataku oraz dostarczać materiały dowodowe (forensics) w postaci min. list adresów URL, IP lub DNS powiązanych z wykrytymi zagrożeniami. 16. Portal WWW musi dostarczać sumaryczne raporty efektywności modułu ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi, identyfikować użytkowników, którzy weszli w bezpośrednią interakcję z wykrytymi przez oprogramowanie zagrożeniami (kliknęli w hiperłącze prowadzące do niebezpiecznej strony malware bądź phishing lub otrzymali wiadomość z niebezpiecznym załącznikiem) oraz tworzyć i stale utrzymywać dynamiczną listę najczęściej atakowanych osób w organizacji Zamawiającego. Lista musi zawierać min. adresy email atakowanych użytkowników oraz wskazywać typy wykrytych ataków (credential phishing / corporate credential phishing / malware / ransomware, RAT, etc.) wraz z ich rozkładem procentowym w rozbiciu na każdego użytkownika ujętego na liście. |
| Funkcjonalność reagowania na wykryte incydenty | 1. W celu wzmocnienia mechanizmów analitycznych oprogramowania ochrony poczty elektronicznej oraz umożliwiania podjęcia automatycznych reakcji na wykryte zagrożenia, oprogramowanie musi zapewniać możliwość integracji z systemem klasy SOAR. Reakcje (działania naprawcze) podejmowane przez system SOAR muszą obejmować przynajmniej możliwość automatycznego usunięcia niebezpiecznych wiadomości dostarczonych na skrzynki odbiorcze użytkowników. System SOAR musi być kompatybilny przynajmniej ze środowiskiem Microsoft Exchange lub Microsoft Office 365. 2. Wskazanie niebezpiecznych wiadomości do usunięcia przez system SOAR musi odbywać się w następstwie zgłoszenia wiadomości przez użytkownika przy użyciu wtyczki alarmującej, dostarczanej jako add-in dla oprogramowania klienta poczty elektronicznej Microsoft Outlook lub w wyniku przesłania kopii wiadomości na monitorowaną przez system SOAR skrzynkę pocztową (tzw. abuse mailbox). Operacja usunięcia wiadomości ze skrzynki odbiorczej użytkownika musi być odwracalna, tzn. musi istnieć możliwość przywrócenia usuniętych wiadomości, np. w przypadku wystąpienia błędów typu false-positive. System SOAR musi zapewniać możliwość powiadomienia użytkownika o usunięciu wiadomości z jego skrzynki odbiorczej, jak również o jej przywróceniu. Powiadomienie musi mieć formę personalizowanej co do treści oraz wyglądu wiadomości email. 3. Zamawiający wymaga dostarczenia wtyczki alarmującej typu add-in dla oprogramowania Microsoft Outlook wraz z oprogramowaniem ochrony poczty elektronicznej, kompatybilnej z oprogramowaniem do ochrony poczty elektronicznej oraz systemem SOAR. 4. Zamawiający wymaga dostarczenia systemu SOAR wraz z oprogramowaniem ochrony poczty elektronicznej. 5. W celu zachowania kompatybilności, system SOAR musi pochodzić od tego samego producenta co oferowane oprogramowanie ochrony poczty elektronicznej oraz oprogramowanie do ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi. |
| Informacje dodatkowe | 1. Administrator musi mieć możliwość zapisu konfiguracji na zewnętrzny nośnik i odtworzenia zapisanej wcześniej konfiguracji. 2. Oprogramowanie musi umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji zgodnie z ustalonym harmonogramem. 3. Wszystkie aktualizacje muszą być pobierane z jednego miejsca a oprogramowanie komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora. 4. Oprogramowanie musi zapewnić śledzenie historii wykonywania aktualizacji. 5. Oprogramowanie musi umożliwiać tworzenie wielu administratorów oraz przypisanie im odpowiednich uprawnień dostępowych do modułów ochronnych. 6. Oprogramowanie musi zapewniać rozbudowany system raportowania zapewniający dostęp do minimum 65 różnych rodzajów graficznych raportów oraz możliwość tworzenia własnych. 7. Oprogramowanie w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych raportów. 8. Administrator musi mieć możliwość okresowej publikacji wybranych raportów jako strony WWW lub przy pomocy wysyłanych automatycznie wiadomości email. 9. Oprogramowanie musi umożliwiać eksport logów do formatu CSV oraz XML. 10. Oprogramowanie musi umożliwiać logowanie na lokalnym dysku twardym lub zewnętrznym serwerze. Oprogramowanie musi mieć możliwość przechowywania logów Syslog, zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji SMTP przez minimum 365 dni. |

1. **Miejsce i termin składania ofert:**
2. Ofertę należy przesłać do dnia **30.11.2022 r. do końca dnia**
3. W celu dołożenia należytej staranności przy ustalaniu szacunkowej wartości planowanego zamówienia, uprzejmie prosimy o podanie ceny netto i brutto, w tym celu należy wypełnić i przesłać formularz ofertowy, stanowiący załącznik nr 1 do Zapytania.
4. Ofertę należy przesłać za pośrednictwem poczty elektronicznej na adres:

[ofertyIT@mrit.gov.pl](mailto:ofertyIT@mrit.gov.pl).

1. **Dodatkowe informacje:**
2. Cena oferty uwzględniająca wszystkie zobowiązania, musi być podana w walucie polskiej, tj. PLN cyfrowo i słownie, z wyodrębnieniem należnego podatku VAT – jeżeli występuje;
3. Cena podana w ofercie powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia;
4. Zapytanie nie jest postępowaniem o udzielenie zamówienia w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Ministerstwa do przyjęcia którejkolwiek z ofert. Złożone przez Wykonawców oferty posłużą wyłącznie przygotowaniu wartości szacunkowej;
5. Ilekroć w niniejszym zapytaniu, przedmiot zamówienia jest opisany ze wskazaniem znaków towarowych, patentów lub pochodzenia, to przyjmuje się, że wskazaniom takim towarzyszą wyrazy „lub równoważne”.