**Załącznik nr 2 do zaproszenia**

## Formularz cenowy

Część nr 2 –**Licencja antywirusowa- rozszerzenie ilościowe**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa towaru** | **Ilość**  **Szt.** | **Cena jedn. netto** | **Wartość netto** | **% VAT** | **Wartość Vat** | **Wartość brutto** | **Nazwa/Producent** |
| 1 | Licencja antywirusowa | 70 |  |  |  |  |  |  |
| 2. | RAZEM | x | x |  | x |  |  | x |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_ r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

podpis osoby(osób)

uprawnionej(ych) do reprezentowania wykonawcy

**Załącznik nr 3 do zaproszenia**

**Część nr 2**

**Licencja antywirusowa- rozszerzenie ilościowe**

**Opis przedmiotu zamówienia (zestawienie granicznych parametrów techniczno-użytkowych )**

|  |  |  |  |
| --- | --- | --- | --- |
| **Licencja źródłowa: ESET PROTECT Enterprise ON-PREM / Ważna do dnia: 2024-01-26 / Obecna liczba stanowisk: 100**  **docelowa liczba stanowisk 170.**  **Specyfikacja oprogramowania docelowego** | | | |
| Lp. | Wymagane minimalne parametry techniczne | Wymóg do spełnienia (warunek graniczny) | OFEROWANE PARAMETRY TECHNICZNE - podaje  Wykonawca  Wymogi dotyczące opisu oferowanych parametrów:  TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający **oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę**  NIE – wykonawca nie spełnia konkretnego parametru |
| **I. Administracja zdalna** | | | |
| **I.** | 1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux  oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie  VHD.  2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera  bazy danych MS SQL i MySQL.  3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera  centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z  modułów oddzielnie bezpośrednio ze strony producenta.  4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku  polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.  5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi  modułami serwera za pomocą certyfikatów.  6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz  dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.  7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.  8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi  modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach  roboczych w sieci.  9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w  tym przynajmniej: producent, model, numer seryjny, informacje o systemie,  procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu,  urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia  masowe).  10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm  trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie  oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.  11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania  do konsoli administracyjnej.  12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i  dynamicznych komputerów.  13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego  warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki  muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan  funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.  14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów,  przygotowanych przez producenta oraz musi zapewniać tworzenie własnych  raportów przez administratora.  15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za  pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.  16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby  każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów,  politykami oraz zadaniami. | TAK |  |
| **II. Ochrona stacji roboczych** | | | |
| **II.** | 1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows  8/Windows 8.1/Windows 10/Windows 11).  2. Rozwiązanie musi wspierać architekturę ARM64.  3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu  adware, spyware, dialer, phishing, narzędzihakerskich, backdoor.  4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami  oraz podłączeniem komputera do sieci botnet.  5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych,  niebezpiecznych oraz podejrzanych aplikacji.  6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych,  zapisywanych i wykonywanych plików.  7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub  pojedynczych plików "na żądanie" lub według harmonogramu.  8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych  oraz dysków sieciowych i dysków przenośnych.  9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania  wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy  kontrolnej (SHA1) oraz lokalizacji pliku.  10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i  IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta  pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta  pocztowego).  11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych  protokołów HTTPS, POP3S, IMAPS.  12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne –  jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne  metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość  wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu  metod jednocześnie.  13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w  tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci  masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń  Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń  przenośnych.  14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup  urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń  minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.  15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  • tryb automatyczny z regułami, gdzie program automatycznie tworzy i  wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych  przez użytkownika,  • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w  przypadku wykrycia aktywności w systemie,  • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone  przez użytkownika,  • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i  użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez  użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie  przełączyć się w tryb pracy oparty na regułach,  • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o  szczególnie podejrzanych zdarzeniach.  16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny  raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:  zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i  sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu  operacyjnego, pliku hosts, sterowników.  17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania  wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić  zagrożenie bezpieczeństwa.  18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika  detekcji.  19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego  korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody  heurystyczne).  20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika  poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed  uruchomieniem systemu operacyjnego.  21. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS  Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.  22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala  tylko na połączenia wychodzące,  • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane  połączenie,  • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i  wychodzący, zezwalając tylko na połączenia skonfigurowane przez  administratora,  • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające  na połączenia przychodzące i wychodzące. Administrator musi posiadać  możliwość konfigurowania czasu działania trybu.  23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.  24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez  Użytkownika.  25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor  ramki przeglądarki oraz informację na ramce przeglądarki.  26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron  internetowych.  27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co  najmniej 140 kategorii i podkategorii.  28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.  29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania  uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych,  klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. | TAK |  |
| **III. Ochrona Serwera** | | | |
| **III.** | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz  Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu  Server 16.04 LTS inowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES)  12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.  2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi  zagrożeniami.  3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu  adware, spyware, dialer, phishing, narzędzihakerskich, backdoor.  4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.  5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne –  jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne  metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć  możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej  lub obu metod jednocześnie.  6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika  detekcji.  7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.  8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie  będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa,  skrypty, dokumenty.  Dodatkowe wymagania dla ochrony serwerów Windows:  9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących  się w usłudze chmurowej OneDrive.  10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście  (HIPS).  11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.  12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika  poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed  uruchomieniem systemu operacyjnego.  13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników  danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci  masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek  USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów  LPT/COM oraz urządzeń przenośnych.  14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i  tworzyć dla nich odpowiednie wyjątki.  15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii  w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.  16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co  najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.  17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup  za pomocą dedykowanego modułu.  Dodatkowe wymagania dla ochrony serwerów Linux:  18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej,  działającej z poziomu przeglądarki internetowej.  19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i  instalacji dodatkowego rozwiązania w postaci usługi serwera Web.  20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni  wspierać rozwiązanie Dell EMC Isilon.  21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.  Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku  awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy  całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. | TAK |  |
| **IV. Szyfrowanie** | | | |
| **IV.** | 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku  Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.  2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w  systemach macOS (FileVault).  3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie  użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także  możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.  4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. | TAK |  |
| **V. Extended Detection and Response** | | | |
| **V.** | 1. Rozwiązanie musi posiadać moduł XDR dla systemów Windows, Linux oraz MacOS  współpracujący z systemem do ochrony stacji roboczych tego samego producenta.  2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu  antywirusowego, tego samego producenta.  3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń  do konsoli administracyjnej tego samego producenta.  4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania  wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.  5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”.  6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące  alarmy, pasujące do utworzonego wykluczenia.  7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o  przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ  podpisu, SHA-1, nazwę komputera, grupę, użytkownika.  8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików  wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego  procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę  firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz  reputację i popularność pliku.  9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych  oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz  ich zablokowania.  10. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej  komentarzy, tagów, nazw reguł.  11. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania  innych administratorów konsoli.  12. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do  stacji roboczej i wykonywania poleceń powershell. | TAK |  |
| **VI. Ochrona urządzeń mobilnych opartych o system Android** | | | |
| **VI.** | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w  pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.  2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i  dokładne.  3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy  urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do  ładowarki).  4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.  5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego  zarządzania, która umożliwi:  a. usunięcie zawartości urządzenia,  b. przywrócenie urządzenie do ustawień fabrycznych,  c. zablokowania urządzenia,  d. uruchomienie sygnału dźwiękowego,  e. lokalizację GPS.  6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych  aplikacji.  7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:  a. nazwę aplikacji,  b. nazwę pakietu,  c. kategorię sklepu Google Play,  d. uprawnienia aplikacji,  e. pochodzenie aplikacji z nieznanego źródła. | TAK |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_ r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

podpis osoby(osób) uprawnionej(ych) do reprezentowania wykonawcy