**Załącznik nr 1a do SIWZ**

**Szczegółowy opis przedmiotu zamówienia dla zadania częściowego nr 1**

1. **Przedmiotem zamówienia jest** 
   1. odnowienie 12-miesięcznej subskrypcji oprogramowania [ESET Endpoint Security](https://sklep.eset.pl/Produkty,pr,37/ESET_Endpoint_Security.html) lub równoważnego do posiadanej licencji dla 2 stanowisk,
   2. odnowienie 12-miesięcznej subskrypcji oprogramowania CODETWO EXCHANGE RULES PRO lub równoważne, na wsparcie techniczne dla 500 użytkowników oraz dostawa 150 nowych licencji oprogramowania CODETWO EXCHANGE RULES PRO lub równoważne wraz   
      z subskrypcją, w
   3. dostawa oprogramowania Trend Micro Deep Security - Anti-malware - per Server (Virtual Machine) lub równoważnego wraz z licencją (30 licencji) oraz 12 miesięczną subskrypcją,
   4. dostawa oprogramowania Trend Micro Deep Security - Anti-malware - per CPU (Socket) lub równoważnego wraz z licencją (12 licencji) oraz 12 miesięczną subskrypcją.
2. **Wymagania Zamawiającego dotyczące przedmiotu zamówienia**
   1. Odnowienie 12 – miesięcznej subskrypcji oprogramowania ESET Endpoint Security lub równoważnego, do posiadanej przez Zamawiającego licencji, dla 2 stanowisk, na nośniku CD lub DVD lub udostępnienie oprogramowania drogą elektroniczną poprzez dostęp do strony internetowej zawierającej dane oprogramowanie oraz dokument potwierdzający prawo do korzystania z programu na wymaganej liczbie stanowisk roboczych wraz z danymi zawierającymi informację umożliwiającą instalację.

Warunki równoważności dla oprogramowania Eset Endpoint Security:

* + 1. Współpraca z centralną konsolą przeznaczoną do zarządzania stacjami, która umożliwia zarządzanie licencjami wdrożonego u Zamawiającego oprogramowania ESET Endpoint Security z poziomu posiadanej przez zamawiającego jednej konsoli ;
    2. Aktualizacja baz definicji wirusów na identycznych zasadach i warunkach technicznych jak aktualizacja wdrożonego u Zamawiającego oprogramowania ESET Endpoint Security;
  1. Odnowienie 12-miesięcznej subskrypcji oprogramowania CODETWO EXCHANGE RULES PRO lub równoważne, na wsparcie techniczne dla 500 użytkowników do posiadanej przez Zamawiającego licencji oraz dostawa 150 nowych licencji wraz z subskrypcją, na nośniku CD lub DVD lub udostępnienie oprogramowania drogą elektroniczną poprzez dostęp do strony internetowej zawierającej dane oprogramowanie oraz dokument potwierdzający prawo do korzystania z programu na wymaganej liczbie stanowisk roboczych wraz z danymi zawierającymi informację umożliwiającą instalację.

Warunki równoważności dla oprogramowania CODETWO EXCHANGE RULES PRO:

* + 1. Podpisy email mogą być tworzone i wdrażane przez administratora dla całej organizacji, w ciągu kilku minut, bez konieczności wprowadzania zmian na każdym komputerze osobno;
    2. Stopki są dodawane pod każdą odpowiedzią lub wiadomością przesyłaną dalej (zamiast na dole korespondencji email);
    3. Obrazki oraz zdjęcia użytkowników Active Directory są dodawane jako ukryte załączniki (brak widocznej ikony załącznika oraz brak konieczności klikania "pobierz obrazy");
    4. Stopki widoczne w folderze Elementy Wysłane;
    5. Edytor stopek HTML dla osób nietechnicznych;
    6. Wymuszenie formatu HTML dla wiadomości plain text;
    7. Wsparcie dla wszystkich klientów pocztowych, urządzeń mobilnych oraz języków;
    8. Automatyczne odpowiedzi, kompresja i usuwanie załączników, DLP
  1. Dostawa 12 (dwunastu) licencji oprogramowania Trend Micro Deep Security - Anti-malware lub równoważne, licencjonowanych w modelu „per-CPU”, obsługujących 12 procesorów fizycznych, zawierających minimum 8 rdzeni na każdy procesor oraz dostawa 30 (trzydziestu) licencji oprogramowania Trend Micro Deep Security - Anti-malware lub równoważne, licencjonowanych w modelu „per-Server”, zwanych dalej Oprogramowaniem AV. Oprogramowanie AV musi zawierać subskrypcje na 12 miesięcy liczone od dnia podpisania protokołu odbioru końcowego.

Warunki równoważności dla oprogramowania Trend Micro Deep Security - Anti-malware:

* + 1. Bieżące, automatyczne identyfikowanie i wyświetlanie aktualnej listy maszyn wirtualnych w konsoli administracyjnej;
    2. Integracja ze środowiskami VMware, Active Directory pozwalająca na odzwierciedlanie aktualnej listy maszyn wirtualnych uruchomionych w wymienionych środowiskach;
    3. Oprogramowanie antywirusowe musi posiadać wsparcie dla środowisk Docker   
       i zapewniać ochronę hostów Docker;
    4. Oprogramowanie antywirusowe musi zapewniać bezpieczeństwo zarówno wirtualnych jak i fizycznych serwerów;
    5. Oprogramowanie antywirusowe musi pozwalać na swobodny wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych oraz zwirtualizowanych desktopów;
    6. W przypadku ochrony w trybie agentowym wszystkie funkcjonalności systemu muszą być dostępne w ramach pojedynczego agenta instalowanego na chronionych obiektach;
    7. Oprogramowanie antywirusowe musi posiadać funkcjonalność automatycznego przypisywania polityk w oparciu o algorytmy zdefiniowane przez administratora, co najmniej w przypadku utworzenia nowego serwera wirtualnego, jego przeniesienia lub zmiany adresacji IP;
    8. Algorytmy w oparciu, o które oprogramowanie antywirusowe przydziela polityki muszą posiadać funkcjonalność definiowania automatycznych działań co najmniej   
       w zależności od:
       1. nazwy serwera;
       2. systemu operacyjnego;
       3. nazwy wykorzystywanego vCenter;
       4. nazwy hosta ESXi;
    9. Funkcjonalność określenia harmonogramu lub częstotliwości pobierania aktualizacji bezpieczeństwa od producenta oprogramowania;
    10. Funkcjonalność zarządzania zdarzeniami i raportowanie – natychmiastowe alarmowanie aktywności wirusów w chronionej sieci;
    11. Oprogramowanie antywirusowe musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów;
    12. Oprogramowanie antywirusowe musi posiadać możliwość pracy w trybie „multi-tenancy”, tj. pozwalać na równoległe współistnienie wielu użytkowników posiadających dostęp do widoku jedynie wydzielonej części infrastruktury i zarządzania jej bezpieczeństwem;
    13. Oprogramowanie antywirusowe musi pozwalać na generowanie raportów   
        z wykorzystania poszczególnych modułów przez użytkowników;
    14. Oprogramowanie antywirusowe musi posiadać funkcjonalność zapewniającą dostęp do konsoli z kilku stacji jednocześnie;
    15. Wszystkie funkcjonalności oprogramowania antywirusowego muszą być zarządzane   
        z tej samej konsoli, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej;
    16. Oprogramowanie antywirusowe musi posiadać wsparcie dla dostępu do konsoli   
        z przeglądarek Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox bez stosowania dodatkowych komponentów lub rozszerzeń;
    17. Oprogramowanie antywirusowe musi umożliwiać personalizację widoku panelu głównego konsoli;
    18. Oprogramowanie antywirusowe musi współpracować z bazami danych Microsoft SQL;
    19. Oprogramowanie antywirusowe musi umożliwiać instalację serwera zarządzającego na systemach Microsoft Windows, RedHat Linux;
    20. Oprogramowanie antywirusowe musi umożliwiać ochronę dystrybucji RedHat Enterprise Linux, CentOS, SUSE Linux, Ubuntu, Debian, AIX;
    21. W zakresie chronionych systemów RedHat Enterprise Linux ochrona powinna zawierać:
        1. Ochronę przed złośliwym oprogramowaniem;
        2. Monitorowanie wybranych procesów;
        3. Monitorowanie wybranych portów;
        4. Analiza ruchu wykorzystującego SSL;
        5. Zmiany w krytycznych oraz wskazanych przez administratora plikach   
           i katalogach;
    22. Funkcjonalność tworzenia kont dla administratorów o różnych stopniach uprawnień   
        w odniesieniu do różnych chronionych maszyn wirtualnych lub ich grup z dokładnością do pojedynczej polityki lub serwera;
    23. Zarządzanie rolami w systemie musi pozwalać zdefiniowanie uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu bez możliwości zmiany nadrzędnego profilu bezpieczeństwa;
    24. Oprogramowanie antywirusowe musi posiadać funkcjonalność tworzenia drzew polityk, w których polityki położone na niższych gałęziach dziedziczą ustawienia   
        z polityk położonych na gałęziach wyższych.
    25. Agentowa i bezagentowa ochrona maszyn wirtualnych w środowisku VMware;
    26. Rozwiązanie powinno pozwalać na powiadamianie użytkownika w przypadku skorzystania z niebezpiecznych zasobów lub pobrania niebezpiecznego pliku, zarówno w trybie agentowym jak i bezagentowym;
    27. Rozwiązanie powinno zapewniać ochronę dla niewspieranych przez ich producentów systemów operacyjnych (Windows XP, Windows 2003);
    28. Oprogramowanie antywirusowe musi posiadać funkcjonalność określenia obszarów skanowania, typów skanowanych plików, momentu ich skanowania (otwarcie i/lub modyfikacja) oraz na wykluczenie ze skanowania określonych obszarów dla skanowania w czasie rzeczywistym, ręcznego skanowania oraz skanowania określonego w harmonogramie;
    29. Określenie reakcji w przypadku wykrycia wirusa;
    30. Oprogramowanie antywirusowe musi zapewniać określenie harmonogramu skanowania (obiekty i grupy) oraz wymuszenia skanowania w danej chwili;
    31. Oprogramowanie antywirusowe musi stosować mechanizm skanowania nowych bądź zmienionych plików w celu skrócenia czasu skanowania oraz zwiększenia wydajności skanowania;
    32. Oprogramowanie antywirusowe musi posiadać funkcjonalność zdefiniowania harmonogramu lub częstotliwości pobierania aktualizacji bazy wirusów, wszelkich poprawek oprogramowania oraz umożliwiać określenie centralnego punktu dystrybucji uaktualnień i poprawek oprogramowania w infrastrukturze zamawiającego;
    33. Oprogramowanie antywirusowe musi posiadać funkcjonalność predefiniowania reakcji w przypadku wykrycia wirusa, w tym co najmniej: czyszczenie, usunięcie, kwarantanna, „false positive”, oraz natychmiastowego automatycznego wykonywania tej reakcji   
        a także raportowania o zdarzeniach w formie co najmniej: e-mail, wiadomość SNMP;
    34. Oprogramowanie antywirusowe musi realizować funkcję hierarchii nadawania uprawnień i delegacji uprawnień administratorów, zarówno dla grup jak   
        i poszczególnych obiektów w szczególności użytkowników, maszyn wirtualnych, ról, polityk, funkcjonalności;
    35. Oprogramowanie antywirusowe musi posiadać funkcjonalność ciągłego, bieżącego   
        i automatycznego wykrywania zagrożeń co najmniej typu: „spyware", „greyware”, „adware", „keylogger”, „dialer”, „trojan”, „malware”;
    36. Oprogramowanie antywirusowe musi posiadać efektywną ochronę przed zagrożeniami typu „ransomware”;
    37. Oprogramowanie antywirusowe musi posiadać mechanizm kontroli aplikacji uniemożliwiający na instalowanie jakichkolwiek niezatwierdzonych do działania   
        w środowisku aplikacji.
    38. Oprogramowanie antywirusowe musi posiadać możliwość otwierania tzw. „okien czasowych”, w których zespoły mogą wprowadzać zmiany do konfiguracji aplikacji na serwerach;
    39. System nie może wymagać restartu chronionych komputerów i serwerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów;
    40. Oprogramowanie antywirusowe musi posiadać funkcjonalność ciągłego, bieżącego   
        i automatycznego blokowania połączeń do adresów URL określonych przez producenta systemu jako niebezpieczne, również w przypadku, gdy połączenia są nawiązywane przez procesy działające na chronionych serwerach, oraz bieżącego aktualizowania listy tych adresów;
    41. Oprogramowanie antywirusowe musi mieć funkcjonalność konfiguracji lokalnego serwera reputacji plików, synchronizującego się z chmurą producenta, który musi zapewniać weryfikację reputacji plików i adresów URL bez konieczności łączenia się   
        z Internetem;
    42. Oprogramowanie antywirusowe musi mieć funkcjonalność definiowania statycznych list adresów URL do których połączenia są ciągle, na bieżąco i automatycznie blokowane przez Oprogramowanie antywirusowe;
    43. Oprogramowanie antywirusowe musi zapewniać ochronę maszyn znajdujących się   
        w strefie DMZ ( ang. demilitarized zone);
    44. Oprogramowanie antywirusowe musi mieć funkcjonalność generowania i wysyłania   
        e-mailem na zdefiniowany adres raportów w wybranym formacie (co najmniej .pdf);
    45. Oprogramowanie antywirusowe musi posiadać funkcjonalność ciągłego, bieżącego   
        i automatycznego identyfikowania i rejestrowania zdarzeń, które wpływają lub mogą wpływać na bezpieczeństwo, wyświetlania listy zdarzeń zidentyfikowanych przez oprogramowanie antywirusowe oraz wg. wyboru administratora automatycznego przekazywania zdarzenia (rozumianego jako wszystkie informacje o zidentyfikowanym przez oprogramowanie antywirusowe zdarzeniu wpływającym na bezpieczeństwo -   
        w formie zbioru informacji (rekordu) do centralnego serwera lub systemu typu SIEM (wg. predefiniowanego wyboru administratora) z wykorzystaniem szyfrowanego kanału komunikacji. W przypadku wysyłania informacji o zdarzeniach do systemu SIEM administrator musi mieć możliwość zdefiniowania centralnego systemu SIEM lub odrębnych systemów dla każdej z polityk, grup chronionych serwerów lub pojedynczych serwerów;
    46. Serwer zarządzający oprogramowania antywirusowego musi posiadać API pozwalające na jego integrację z zewnętrznymi systemami zarządzającymi firm trzecich. Dokumentacja API zapewniająca integrację z zewnętrznymi systemami zarządzającymi firm trzecich musi być powszechnie dostępna;
    47. Oprogramowanie antywirusowe musi mieć funkcjonalność tworzenia ról administratorów i przydzielania im uprawnień co najmniej w zakresie zarządzania:
        1. Serwerami lub grupami serwerów;
        2. Politykami lub grupami polityk;
        3. Poszczególnymi funkcjonalnościami Oprogramowania antywirusowego;
    48. Oprogramowanie antywirusowe musi mieć funkcjonalność tworzenia logicznych grup serwerów w celu zarządzania tymi grupami oraz wymuszania stosowania określonych dla grup zasad bezpieczeństwa, ustanawianych dla każdej z grypy indywidulanie;
    49. Oprogramowanie antywirusowe musi mieć funkcjonalność tworzenia drzewa polityk zależnych, w którym polityki pochodne dziedziczą ustawienia od polityk na wyższym poziomie. Administratorzy posiadający uprawnienia jedynie do polityk pochodnych nie mogą mieć możliwości wprowadzania zmian do ustawień dziedziczonych.
  1. Za produkty dostarczane w ramach wsparcia producenta w czasie jej trwania Zamawiający nie będzie ponosił dodatkowych kosztów.
  2. Minimum jednodniowy warsztat powdrożeniowy prowadzony przez certyfikowanego inżyniera zgodnie z wymaganiami określonymi w pkt 6.

1. **Harmonogram realizacji.**
   1. W terminie wskazanym w ofercie (nie później niż 14 dni od dnia podpisania umowy) Wykonawca dostarczy niezbędne licencje zgodnie z wymaganiami Zamawiającego i złożoną ofertą. Dostawa zostanie potwierdzona podpisaniem Protokołu Odbioru Dostawy.
   2. W terminie wskazanym w ofercie (nie później niż 30 dni od dnia dostarczenia oprogramowania) Wykonawca:
      1. Przeprowadzi instalacje i konfigurację dostarczonego Oprogramowania AV.
      2. Skonfiguruje i zoptymalizuje dostarczone oprogramowanie AV do współpracy   
         z posiadanym przez Zamawiającego oprogramowaniem.
      3. Usunie dotychczas wykorzystywane oprogramowanie antywirusowe ESET File Security zainstalowane na serwerach.
      4. Dostarczy szczegółową dokumentację powykonawczą oraz procedury eksploatacyjne i awaryjne zgodnie z wymaganiami określonymi w pkt 4. Zakres dokumentacji i procedur zostanie uzgodniony wcześniej z Zamawiającym.
      5. Przeprowadzi co najmniej jednodniowy (zgodnie ze złożoną ofertą) warsztat powdrożeniowy zgodnie z wymaganiami określonymi w pkt 6, dokładny termin,   
         w którym zostanie przeprowadzony warsztat powdrożeniowy należy uzgodnić
      6. z Zamawiającym.
      7. Zakończenie wdrożenia zostanie potwierdzone podpisaniem Protokołu Odbioru Wdrożenia.
2. **Minimalne wymagania Zamawiającego dotyczące dostarczonej dokumentacji instalacji, konfiguracji i parametryzacji oprogramowania AV.**
   1. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji umowy charakteryzowały się wysoką jakością, w szczególności:
      1. Czytelną i zrozumiałą strukturą zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały podrozdziały i sekcje.
      2. Zachowaniem standardów oraz sposobu pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, oraz fragmentów tego samego dokumentu jak również całej dokumentacji.
   2. Wykonawca przygotuje w szczególności:
      1. Procedury i instrukcje dotyczące instalacji konfiguracji oraz parametryzacji wdrożonego oprogramowania.
      2. Procedury i instrukcje wykonania kopii bezpieczeństwa i ich odtworzenia.
      3. Procedury i instrukcje aktualizacji i wdrażania poprawek.
      4. Procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji i rozwiązywania zaistniałych problemów,
   3. Każda z procedur powinna zawierać co najmniej następujące dane:
      1. Nazwa.
      2. Opis.
      3. Częstotliwość wykonywania.
      4. Kroki do zrealizowania w procedurze.
      5. Informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce) na jakie należy zwrócić uwagę w trakcie wykonywania procedury.
      6. Omówienie zawartości komunikatów jeśli są prezentowane.
      7. Kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.
   4. Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji.
3. **Minimalne wymagania Zamawiającego w zakresie świadczenia usług wsparcia technicznego producenta oprogramowania.**
   1. Wsparcie techniczne producenta musi obejmować minimum;
      1. Konsultacje telefonicznych/mailowe w dni robocze w godz. 8:00- 17:00,
      2. Zapewnienie dostępu do systemu obsługi zgłoszeń serwisowych SUPPORT (serwis www/mail),
      3. Zapewnienie dostępu do poprawek i aktualizacji Oprogramowania,
      4. Zapewnienie dostępu do sygnatur i silników złośliwego oprogramowania,
      5. Zapewnienie dostępu do bazy wiedzy o produkcie.
      6. Świadczenie pomocy technicznej musi być realizowane bez ograniczeń co do ilości zgłoszeń.
4. **Minimalne wymagania stawiane przez Zamawiającego w zakresie warsztatu powdrożeniowego oprogramowania AV.**
   1. Z wdrażanego u Zamawiającego rozwiązania Wykonawca zorganizuje warsztat powdrożeniowy, który będzie prowadzony przez certyfikowanego inżyniera zaoferowanego rozwiązania, z zakresu administracji wdrożonego oprogramowania AV, dla jednej grupy administratorów liczącej do 8 osób, w siedzibie Zamawiającego w Warszawie przy   
      ul. Koszykowej 16 lub Taborowej 33.
   2. Termin warsztatu zostanie uzgodniony z Zamawiającym z co najmniej siedmiodniowym wyprzedzeniem.
   3. Program warsztatu musi obejmować całość zagadnień związanych z czynnościami administracyjnymi z zakresu administrowania wdrożonym Oprogramowaniem AV uwzględniając środowisko produkcyjne Zamawiającego i następującą tematykę:
      1. podstawowa i zaawansowana konfiguracja i administracja Oprogramowaniem AV,
      2. proces monitoringu i raportowania wdrożonego Oprogramowania AV
      3. proces zarządzania zmianami konfiguracyjnymi Oprogramowania AV,
      4. diagnozowanie i rozwiązywanie problemów związanych z wdrożonym Oprogramowaniem AV.
   4. Program warsztatu musi być zgodny z wersją wdrożonego rozwiązania i obejmować omówienie najczęściej występujących awarii oraz sposoby ich usuwania i zabezpieczania się przed nimi.
   5. Warsztat musi trwać minimum 1 dzień roboczy, 6 godzin efektywnych zajęć. Wykonawca może zaoferować przeprowadzenie warsztatu w rozbudowanej, 2-dniowej formule uzgodnionej przed jego rozpoczęciem z Zamawiającym. Rozbudowany 2 dniowy warsztat jest traktowany jako dodatkowe kryterium oceny ofert.
   6. Wykonawca zapewni uczestnikom warsztatu materiały szkoleniowe w formie papierowej   
      i elektronicznej.
5. **Minimalne wymagania Zamawiającego dotyczące świadczenia usług wynikających z udzielonej gwarancji na oprogramowanie AV.**
   1. Wykonawca udziela gwarancji na prawidłowe, w pełni zgodne z jego przeznaczeniem, funkcjonowanie Oprogramowaniem AV objętego wsparciem technicznym producenta, przez okres 12 miesięcy, tj. od dnia podpisania protokołu odbioru końcowego.
   2. Czas usunięcia nieprawidłowości wskazanych w zgłoszeniu gwarancyjnym wynosi do 5 dni roboczych od daty zgłoszenia gwarancyjnego pod rygorem naliczania kar umownych na zasadach określonych w Umowie i może ulec wydłużeniu wyłącznie za pisemną zgodą Zamawiającego w przypadku wystąpienia okoliczności niezależnych od Wykonawcy   
      i Zamawiającego.
   3. Udzielone gwarancje nie mogą ograniczać praw Zamawiającego do użytkowania wdrożonego oprogramowania, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego.