Załącznik nr 1 Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest:

   a) Dostawa oprogramowania do ochrony antywirusowej dla stacji roboczych lub oprogramowania równoważnego zgodnie z tabelą w punkcie 3.
   b) Dostawa oprogramowania do wykrywania oraz reagowania na zagrożenia na stacjach końcowych typu EDR (Endpoint Detection and Response), lub XDR (Extended Detection and Response) dla stacji lub oprogramowania równoważnego zgodnie z tabelą w punkcie 3.
   c) Dostawa systemu zarządzania oprogramowaniem na stacjach roboczych (konsola) lub oprogramowania równoważnego zgodnie z wymaganiami ilościowymi określonymi w tabeli w punkcie 3.
   d) Migracja oprogramowania na stacjach roboczych oraz serwerach wskazanych przez Zamawiającego.

   e) zapewnieniu wsparcia merytorycznego i pomocy technicznej w zakresie:
      i. rozwiązywania problemów wynikłych w trakcie instalacji i konfiguracji najnowszej wersji oprogramowania objętego licencjami dostarczonymi/udzielonym przez Wykonawcę zgodnie z potrzebami i zaleceniami Zamawiającego,
      ii. rozwiązywania problemów wynikłych w trakcie użytkowania oprogramowania objętego licencjami dostarczonymi/udzielonymi przez Wykonawcę oraz pomoc w usuwaniu wad/błędów tego oprogramowania poprzez sygnalizowanie producentowi oprogramowania konieczności podjęcia stosownych kroków (np. wydania nowej wersji oprogramowania, wydania łatki (patch)) usuwającej stwierdzone wady/błędy.
2. Rozwiązanie nie może być wymienione w rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa o niestosowaniu oprogramowania.
3. Wymagania ilościowe:

Oprogramowanie	Ilość licencji	Data rozpoczęcia	Data zakończenia
Oprogramowanie antywirusowe	5210	14.01.2024	13.01.2027
Oprogramowanie EDR/XDR	350	14.01.2024	13.01.2027
Oprogramowanie antywirusowe (Opcje)	1000	Uruchomienie opcji zgodnie z par 2 ust 2 Umowy	13.01.2027
Oprogramowanie EDR/XDR (Opcje)	100	Uruchomienie opcji zgodnie z par 2 ust 2 Umowy	13.01.2027

4. Wymagania minimalne dla Systemu:
   a) Zamawiający aktualnie posiada oprogramowanie Eset Endpoint Security Eset oraz Endpoint Antyvirus oraz Eset Inspect wraz z

konsolami zarządzania ESET Protect&Inspect i wymaga żeby poziom dostarczonego oprogramowania był taki sam, lub równoważny.

b) Serwery zarządzające – zasoby:
   - ESET Protect Server (virtual appliance)– 6 CPU, 64 GB HDD, 20 GB RAM
   - ESET Inspect Server – 6 CPU, 60 GB HDD, 8 GB RAM, Windows Server 2019 64-bit, MS SQL 2019

Ochrona stacji roboczych - specyfikacja równoważna

1. Rozwiązanie musi wspierać systemy operacyjne Windows7 /Windows8 /Windows8.1 /Windows10/ Windows 11, Mac OS X (systemy 32 i 64 bitowe) oraz posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim wraz z dokumentacją.
3. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami, oraz musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. Musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
   Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
   Rozwiązanie musi zapewniać automatyczne usuwanie wirusów oraz alarmować w przypadku wykrycia zagrożenia.
4. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików oraz pozwalać na skanowania całego dysku (lokalnego komputera, sieciowego oraz przenośnego), wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.

   Dodatkowo musi pozwalać na:
   a. Skanowanie plików skompresowanych z możliwością ustawienia poziomu przy wielokrotności kompresji lub/i wielkości pliku skompresowanego,
   b. Tworzenie listy wykluczeń ze skanowania wybranych plików katalogów lub o określonych rozszerzeniach
   c. Okresowe skanowanie, które ma odbywać na podstawie przygotowanych przez producenta harmonogramów lub utworzonych przez administratora. Musi być możliwości ustawienia rozpoczęcia skanowania na podstawie określenia czasu rozpoczęcia skanowania lub na podstawie stanu stacji roboczej tj. stacja uruchomiona – użytkownik zablokował

stację (Windows+L), uruchomienia wygaszacza ekranu, stacja uruchomiona użytkownik niezalogowany.
   d. Automatyczne natychmiastowe skanowanie podłączonego nośnika zewnętrznego.
   e. Ochronę przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
   f. ochronę przed oprogramowaniem wymuszającym okup.
5. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" oraz ruchu HTTP (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego lub przeglądarki. Rozwiązanie musi się integrować z dowolnym klientem poczty i dowolną przeglądarką bez konieczności wprowadzani zmian w ich konfiguracji. Dodatkowo musi pozwalać na skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
6. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
9. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
10. Funkcjonalność Host IPS (Host Intrusion Prevention System) dla stacji końcowych użytkowników musi chronić systemy użytkowników przed znanymi podatnościami za pomocą dostarczanych przez producenta sygnatur.
11. Funkcjonalność Host IPS musi wykrywać skanowania portów, chronić przed atakami sieciowymi, oraz wykorzystującymi znane podatności aplikacji oraz systemów operacyjnych.
12. Rozwiązanie musi posiadać możliwość wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu w trybie automatycznym lub na polecenie użytkownika. Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. Musi istnieć możliwość wysyłania próbek bezpośrednio z kwarantanny. Zbierane przez producenta, na podstawie otrzymanych próbek nowych zagrożeń, dane mają być w pełni anonimowe.
13. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
14. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku

aktualizacji – poinformować o tym użytkownika, co najmniej o kategorii aktualizacji tj. aktualizacje krytyczne, aktualizacje ważne i zalecane. Musi być możliwość wyłączenia tego mechanizmu kontroli.

15. Rozwiązanie musi posiadać, umożliwiać administratorowi kontrolowanie 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. Blokowanie musi się odbywać na podstawie reguł w oparciu o grupy urządzeń, typu, numeru seryjnego, identyfikatora USB, producenta i modelu urządzenia. Zakres nadawanych dostępów musi pozwalać na:
    a. Pełen dostęp do urządzenia
    b. Dostęp w trybie tylko do odczytu
    c. Odmowa dostępu.
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, ostatniego połączenia do systemu zarządzania, daty ostatniego skanowania.
17. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
    Musi pozwalać na:
    d. utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
    e. określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
    f. tworzenia lokalnego repozytorium aktualizacji modułów.
    g. tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
    h. Tworzenie lub przygotowanie aktualizacji dla stacji odłączonych od sieci, pracujących w trybie off-line wraz z możliwością przegrania jej na pamięć zewnętrzną
19. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
20. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

21. Musi pozwalać na kolekcjonowanie danych z klienta nawet w przypadku utraty połączenia z konsolą administracyjną oraz automatycznie je przesyła po odzyskaniu połączenia.
22. Rozwiązanie musi posiadać zaporę osobistą, rozwiązanie musi pracować w jednym z czterech trybów:
    a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

    Dodatkowo musi:
    - oceniać reguły zapory systemu Windows
    - pozwalać na tworzenie listy sieci zaufanych
    - pozwalać na pełne wyłączenie funkcji zapory osobistej
23. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

Ochrona stacji roboczych - zarządzanie
specyfikacja równoważna

1. Zarządzanie klientami ma odbywać się przez dedykowana konsolę administracyjną tego samego producenta co oprogramowanie Antywirusowe. Zarządzanie może odbywać się poprzez dedykowanego Agenta lub bezpośrednio z klientem antywirusowym tego samego producenta.
2. Serwer konsoli administracyjnej musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych w środowisku wirtualnym lub jako dedykowane urządzenie wirtualne. Serwer musi pracować na zasobach Zamawiającego.
3. Serwer konsoli administracyjnej musi wspierać instalację z wykorzystaniem wbudowanej w rozwiązanie bazy danych lub istniejącego serwera bazy danych MS SQL lub MySQL.
4. Dostęp do konsoli administracyjnej zabezpieczony za pośrednictwem protokołu SSL.
5. Komunikacja pomiędzy klientami/agentami a konsolą administracyjną musi być szyfrowana i bezpieczna.
6. Rozwiązanie musi mieć możliwość integracji z MS Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów.

7. Rozwiązanie musi umożliwiać tworzenie ról administratorów o różnych stopniach uprawnień i dostępów.
8. Konsola administracyjna musi pozwalać na pełną konfigurację uruchomionych i zainstalowanych klientów włącznie z deinstalacją klientów lub/i agentów.
9. Konsola administracyjna musi być wyposażona w funkcję tworzenia raportów z danych przesłanych od klientów, pozwalać na tworzenie zestawień na podstawie jednego lub wielu pól danych otrzymanych od klienta antywirusowego/agenta oraz zapewnić możliwość generowania wykresów/diagramów/zestawień (logiczne filtrowanie informacji).
10. Musi być możliwość eksportu raportowanych danych co najmniej do formatu PDF i CSV wraz z możliwością utworzenia harmonogramów wysyłki raportów pocztą elektroniczną.
11. Musi pozwalać na wykonywanie harmonogramu i wysyłki raportów poprzez pocztę elektroniczną.
12. Musi pozwalać na pełne zarządzanie stacjami z zainstalowanym klientem antywirusowym/agentem poprzez skategoryzowane szablony zadań oraz pozwalać na tworzenie nowych zadań w ramach danej kategorii
13. Musi pozwalać na wysyłanie komend do systemu operacyjnego, co najmniej: wyłącz komputer, uruchom ponownie komputer, wyloguj, zainstaluj aktualizacje systemowe.
14. Konsola administracyjna musi mieć możliwość tagowania obiektów.
15. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
16. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
17. Konsola administracyjna musi pozwalać na grupowanie stacji oraz przypisywanie do grup określonych konfiguracji klientów. Hierarchiczna budowa grup musi pozwalać na dziedziczenie konfiguracji z grup od pierwszej grupy do najbardziej zagnieżdżonej.
18. Konsola administracyjna musi pozwalać na przyjmowanie połączeń klientów pracujących poza siecią Zamawiającego poprzez serwer pośredniczący tego samego producenta. Serwer pośredniczący musi mieć możliwość pobierania aktualizacji sygnatur oraz aktualizacji oprogramowania klienta antywirusowego oraz przechowywania ich do dalszej dystrybucji.
19. Rozwiązanie musi umożliwiać integrację z systemem SIEM lub zewnętrznym kolektorem logów.

Ochrona stacji roboczych – licencje specyfikacja równoważna

1. Zarządzanie licencjami oferowanego oprogramowania musi odbywać się poprzez portal licencji producenta.
2. Sposób licencjonowania musi pozwalać na automatyczne zwalnianie licencji, gdy klient nie podłączy się do portalu licencji producenta.

Portal musi pozwalać na ustawienie czasu, po jakim licencja zostanie zwolniona.
3. Portal musi pozwalać na tworzenie kont administratorów z różnymi zakresami uprawnień.
4. Portal powinien pozwalać na przydzielanie licencji do samodzielnego zarządzania dla poszczególnych administratorów licencji z puli Zamawiającego.

EDR/XDR - specyfikacja równoważna

1. Rozwiązanie musi wspierać systemy operacyjne Windows7 (minimum do końca 2024 roku) /Windows8 /Windows8.1 /Windows10/ Windows 11, Mac OS X (systemy 32 i 64 bitowe) oraz posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim wraz z dokumentacją.
3. Oferowany system EDR/XDR musi współpracować z klientem Antywirusowym i pochodzić od tego samego producenta.
4. Konsola zarządzania może być zintegrowana z konsolą administracyjną klienta antywirusowego lub być osobną konsolą korzystającą z danych konsoli zarządzania programem antywirusowym. Integracja danych musi odnosić się co najmniej do struktury grup komputerów, kont administratorów oraz uprawnień oraz aktualizacji.
5. Serwer konsoli administracyjnej musi posiadać możliwość instalacji na systemach wirtualnych Windows Server 2012 i nowszych w środowisku wirtualnym lub jako dedykowane urządzenie wirtualne. Serwer musi pracować na zasobach Zamawiającego.
6. Sposób licencjonowania jak i zarządzania licencjami musi być zgodny z zarządzaniem licencjami klienta antywirusowego.
7. Oferowany system klasy EDR/XDR musi posiadać możliwość zbierania danych z różnych warstw środowiska IT, w tym co najmniej z:
   a. Stacji końcowych i serwerów. Niniejsze zapytanie obejmuje funkcjonalności zbierania danych ze stacji końcowych pracowników.
   b. Dane zbierane ze stacji końcowych powinny obejmować co najmniej:
      - Procesy, w tym modyfikacja
      - Pliki
      - Połączenia sieciowe
      - Zapytania DNS
      - Rejestry
      - Konta i użytkownicy
      - Zdarzenia Internetowe (obsługa URL)

- Windows hooks
- Detekcje i zdarzenia bezpieczeństwa

8. Dane zbierane z poszczególnych warstw muszą być normalizowane i korelowane między sobą.
9. W wyniku korelacji system musi tworzyć detekcje zagrożeń w klasyfikacji: zagrożenie - wysoki, ostrzeżenie – średni, informacyjny – niski.
10. Dane muszą być mapowane na matrycę TTP (techniques, takctiques, procedures), z uwzględnieniem matrycy MITRE ATT&CK.
11. System musi pozwalać na wyeksportowanie wybranych zdarzeń w formacie CSV lub JSON
12. Wszelka aktywności w systemie musi być zapisywana i ewidencjonowana z zapewnieniem odpowiedniej rozliczalności działań analityków w środowisku
13. Threat Intelligence – system musi dostarczać i integrować dane zebrane przez producenta o zagrożeniach i kampaniach przestępczych
14. System musi posiadać możliwość tworzenia automatycznie i manualnie wyzwalanych akcji w oparciu z wcześniej zdefiniowane kryteria – tzw. „Playbook”
15. Tworzenie playbook’ów musi być oparte o schemat blokowany i nie musi wymagać jakiejkolwiek wiedzy programistycznej czy związanej z pisanej skryptów
16. System musi wskazywać jaki zasięg ma dany alert – ile i jakie serwery/stacje/użytkownicy są powiązani z alertem
17. System ma pozwalać na zarządzanie statusem alertu:
    a. Nowy (New - status domyślny)
    b. W trakcie realizacji (in progress)
    c. Zamknięty (closed)
    d. False Positive (closed – False Positive)
18. Z alertów administratorzy muszą mieć możliwość tworzenia Incydentów w których mogą opisywać podjęte działania.
19. System musi pozwalać na tworzenie listy obiektów do zablokowania/listy wyjątków
20. System musi pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji roboczej/serwera system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą.
21. System musi być oparty o wydajny silnik analityczny pozwalający na pracę z danymi bez zbędnej zwłoki.
22. Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy)