Załącznik nr 1
do Zapytania Ofertowego

Opis przedmiotu zamówienia

1. Przedmiot zamówienia

Zakup licencji na oprogramowanie antywirusowe z modułem zarządzania podatnościami oraz incydentami oraz modułem zapory osobistej dla 250 użytkowników na okres 24 miesięcy.

2. Wymagania funkcjonalne

1) Oprogramowanie i licencje muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego.
2) Licencjonowanie musi uwzględniać (w okresie obowiązywania gwarancji) prawo do bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych
3) Licencjonowanie musi uwzględniać prawo do najnowszej wersji zakupionego produktu przez cały okres obowiązywania gwarancji.
4) Licencjonowanie musi uwzględniać prawo do pobierania najnowszej bazy sygnatur wirusów na stacjach końcowych przez cały okres obowiązywania gwarancji.
5) Oprogramowanie nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
6) Zintegrowana zapora sieciowa (firewall) dla zabezpieczenia ruchu sieciowego.
7) Regularne aktualizacje baz sygnatur wirusów oraz komponentów programu.
8) Możliwość centralnego zarządzania ochroną i konfiguracją z poziomu panelu administracyjnego w min. 2 lokalizacjach.
9) Licencja na 250 użytkowników na okres 24 miesięcy z możliwością przenoszenia pomiędzy komputerami.
10) Możliwość aktywacji poprzez połączenie internetowe.
11) Licencja obejmuje dostęp do aktualizacji oraz wsparcia technicznego.
12) Obsługa zarządzania zdalnego w systemach Windows Server oraz Linux.
13) Możliwość wdrożenia rozwiązania jako maszyna wirtualna.
14) Wsparcie techniczne w języku polskim dostępne dla posiadaczy licencji.
15) Dostępność dokumentacji technicznej oraz instrukcji instalacji.
16) Możliwość integracji z istniejącą infrastrukturą IT organizacji.
17) Ochrona urządzeń mobilnych z Android

3. Konsola centralnego zarządzania

1) Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
2) Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
3) Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
4) Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
5) Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
6) Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

7) Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania:
    a) politykami,
    b) raportowaniem,
    c) zarządzaniem licencjami,
    d) zadaniami administracyjnymi.
8) Każda z funkcji musi posiadać możliwość wyboru uprawnienia:
    a) odczyt,
    b) użyj,
    c) zapisz,
    d) brak.
9) Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10) Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11) 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:
    a) adresy sieciowe IP,
    b) aktywne zagrożenia,
    c) stan funkcjonowania/ochrony,
    d) wersja systemu operacyjnego,
    e) podzespoły komputera.
12) Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem:
    a) wyrażenie CRON,
    b) codziennie,
    c) cotygodniowo,
    d) comiesięcznie,
    e) corocznie,
    f) po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

4. Ochrona stacji roboczych

1) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2) Rozwiązanie musi wspierać architekturę ARM64.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Rozwiązanie musi posiadać funkcjonalność przywrócenie plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
6) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
7) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

8) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
10) 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.
11) Rozwiązanie musi integrować się z Intel Threat Detection Technology.
12) 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).
13) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
14) 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.
15) 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.
16) 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.
17) Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d) 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.
18) 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.

19) 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.
20) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
21) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
22) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23) Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
24) Zapora osobista rozwiązania 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.
25) Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
26) Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
27) Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
28) Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
29) Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
30) Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
31) 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.

5. Ochrona serwera

1) Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Ubuntu, Debian, SUSE Linux Enterprise Server (SLES).
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, narzędzi hakerskich, 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.

6. Moduł szyfrowania

1) System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
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.
5) Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO).

7. Ochrona urządzeń mobilnych opartych o system Android

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.

8. Aktualizacja baz danych sygnatur zagrożeń

1) Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
2) Program powinien posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
3) Program powinien posiadać możliwość określenia źródła uaktualnień.
4) Program powinien posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.
5) Program powinien posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
6) Program powinien posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
7) Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).

9. Sandbox w chmurze

1) Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2) Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3) Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4) Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5) Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6) Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7) Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8) Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9) Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10) Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11) Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12) Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a) czysty,
    b) podejrzany,
    c) bardzo podejrzany,
    d) szkodliwy.

13) W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania
14) pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
15) W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
16) Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

10. Moduł XDR

1) Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2) Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3) Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4) Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5) Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6) Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7) Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8) Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9) Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10) Administrator musi posiadać możliwość weryfikacji 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.
11) Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12) Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13) W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14) W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość
15) weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

16) Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej.
17) W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej:
    a) podzespołów zarządzanego komputera, w tym przynajmniej:
    b) producent,
    c) model,
    d) numer seryjny,
    e) informacje o systemie,
    f) procesor,
    g) pamięć RAM,
    h) wykorzystanie dysku twardego,
    i) informacje o wyświetlaczu,
    j) urządzenia peryferyjne,
    k) urządzenia audio,
    l) drukarki,
    m) karty sieciowe,
    n) urządzenia masowe. oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
18) Konsola administracyjna musi mieć możliwość tagowania obiektów.
19) Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

11. Wsparcie i asysta techniczna.

1) W całym okresie trwania subskrypcji (ważności klucza licencyjnego) użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
2) W całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej.
3) Dostęp do dokumentacji i instruktaży on-line/webinariów dot. aktualnie użytkowanych wersji.
4) Aktualizacja baz danych sygnatur zagrożeń na bieżąco podczas trwania wartości klucza licencyjnego.