OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest odnowienie licencji dla obecnie użytkowanego oprogramowania ESET PROTECT Entry zapewniającego ochronę antywirusową dla 10 000 użytkowników na okres 12 miesięcy (od 1.01.2027 r. do 31.12.2027 r.)

1. Przedmiotem umowy jest zakup i dostawa do siedziby Zamawiającego licencji na oprogramowanie antywirusowe do obecnie użytkowanego oprogramowania ESET PROTECT Entry (licencja 3AC-5V2-7PN), zapewniającego ochronę antywirusową dla 10 000 użytkowników sądów apelacji łódzkiej na okres 12 miesięcy.

2. Na Przedmiot umowy określony w ust. 1 składają się następujące czynności:
   sprzedaż i dostarczenie przez Wykonawcę do siedziby Zamawiającego dokumentów licencyjnych (certyfikat licencyjny) kodów/ kluczy, informacji umożliwiających dostęp do portalu służącego do zarządzania licencją, potwierdzających legalne nabycie przez Zamawiającego licencji, wraz z wymaganą dokumentacją dla Przedmiotu umowy zgodnie z poniższą specyfikacją:
   - obecne licencje (10 000 szt.) obowiązują do 31.12.2026 r. Zamawiający wymaga uruchomienia licencji od dnia 01.01.2027 r.;
   - liczba i rodzaj licencji oraz okres obowiązywania mają być widoczne na koncie Zamawiającego w systemie zarządzania licencjami Wykonawcy;
   - przed podpisaniem Umowy Wykonawca dostarczy dokument zawierający warunki wsparcia Producenta, który zostanie dołączony do umowy jako załącznik;
   - podstawowy zakres obowiązków Wykonawcy ogranicza się wyłącznie do dostarczenia licencji oraz świadczenia standardowego wsparcia technicznego producenta;

Wymagania dotyczące bezpieczeństwa Oprogramowania:

1. Oprogramowanie wykorzystywane do świadczenia Usługi nie może być zabronione do stosowania przez administrację któregokolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).
2. Oprogramowanie wykorzystywane do świadczenia Usługi nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).

W przypadku zaoferowania produktu równoważnego, do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.
Koszt licencji produktu równoważnego (w ilości 10 000 stanowisk) obejmuje wyłącznie dostarczenie prawa do korzystania z oprogramowania oraz aktywację.
Usługi techniczne związane z procesem migracji środowiska Zamawiającego na produkt równoważny nie są objęte przedmiotem zamówienia. Wykonawca nie jest zobowiązany do świadczenia bezpłatnych usług migracyjnych.
Użytkownik / licencja stanowiskowa – należy przez to rozumieć jednostkę licencjonowania zgodną z oficjalnym cennikiem i metryką licencjonowania producenta oferowanego uprawniającą 1 unikalnego użytkownika (lub 1 dedykowane konto/stanowisko) do korzystania z oprogramowania. Zamawiający wymaga dostarczenia 10 000 takich jednostek.
Zamawiający dopuszcza zaoferowanie produktu równoważnego, spełniającego następujące wymagania:

Centralne zarządzanie

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania.
4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
5. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID. 6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
7. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:
    - Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
    - Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
    - Buforowanie ruchu HTTPS.
9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    - Google Authenticator,

- Microsoft Authenticator,
- Authy,
- Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.

12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
14. 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 oraz ochrony.
    - Wersja systemu operacyjnego.
    - Podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    - Wyrażenie CRON.
    - Codziennie.
    - Cotygodniowo.
    - Co miesiąc.
    - Co rok.
    - Po wystąpieniu nowego zdarzenia.
    - Po automatycznym umieszczeniu hosta w grupie dynamicznej.
16. Rozwiązanie musi udostępniać możliwość tagowania obiektów.
17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
    - JSON.
    - LEEF.
    - CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan.
    - Robak.

- Adware.
- Spyware
- Dialer.
- Phishing.
- Backdoor.

4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
8. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
9. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    - Całego dysku.
    - Wybranych katalogów.
    - Pojedynczych plików.
    - Plików spakowanych oraz skompresowanych.
    - Dysków sieciowych.
    - Dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - Wybranych plików.
    - Wybranych procesów. ➢ Wybranych lokalizacji.
    - Wybranych rozszerzeń.
    - Nazwy wykrycia.
    - Sumy kontrolnej (SHA1).
11. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
12. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

- Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

13. Rozwiązanie musi udostępniać 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).
14. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
15. Rozwiązanie musi udostępniać 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
16. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

    A. Typ urządzenia:

    - Pamięci masowe.
    - Optyczne pamięci masowe.
    - Pamięci masowe Firewire.
    - Urządzenia do tworzenia obrazów.
    - Drukarki USB.
    - Urządzenia Bluetooth.
    - Czytniki kart inteligentnych.
    - Modemy.
    - Porty LPT/COM.
    - Urządzenia przenośne.

    B. Parametry urządzenia:

    - Numer seryjny.
    - Producent.
    - Model. C. typ dostępu:
    - Brak możliwości zapisu.
    - Pełen dostęp.
    - Ostrzeżenie użytkownika.
    - Brak dostępu.

17. Rozwiązanie musi udostępniać moduł HIPS, który 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.

18. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    A. 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.
    B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. C. Raport musi posiadać co najmniej:
        - Listę zainstalowanych aplikacji.
        - Listę usług systemowych.
        - Informacje o systemie operacyjnym i sprzęcie.
        - Listę aktywnych procesów i połączeń sieciowych.
        - Harmonogram systemu operacyjnego.
        - Szczegóły pliku hosts.
        - Informacje o sterownikach.
19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu ➢ Antywirus.

- Zapora osobista.
- Sandbox.
- 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 realizowaną przez dedykowaną wtyczkę.
    A. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
    B. Ochrona musi być realizowana w oparciu o co najmniej:
        - globalna czarna lista RBL,
        - czarna lista użytkownika,
        - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
22. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - Skanowanie portów TCP oraz UDP,
        - Wykrywanie duplikacji adresu IP,
        - Atak zatruwania ARP,
        - Nieprawidłowa długość pakietu TCP oraz UDP.
    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        - RDP,
        - SMB,
        - My SQL,
        - MS SQL.
    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
23. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    B. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

24. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
    - Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
    - Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor
    - ramki przeglądarki oraz informację na ramce przeglądarki.
    - W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
25. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
    A. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
    B. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
        - Treść komunikatu.
        - Obraz.

Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan. ➢ Robak.
    - Adware.
    - Spyware. ➢ Dialer.
    - Phishing.
    - Backdoor.
4. 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.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
   - Sygnatur wirusów.
   - Reputacji chmurowej.
7. Rozwiązanie musi umożliwiać 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).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku,
   - wybranych katalogów,
   - pojedynczych plików,
   - plików spakowanych oraz skompresowanych,
   - Dysków sieciowych,
   - dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
    - nazwy wykrycia,
    - sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
    B. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
        - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
    - Ubuntu Desktop,
    - Red Hat Enterprise Linux
    - Linux Mint.
2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
    - Cinnamon.
    - GNOME.
    - KDE.
    - MATE.
    - XFCE.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan. ➢ Robak.
    - Adware.
    - Spyware. ➢ Dialer.
    - Phishing.
    - Backdoor.
4. 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.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - Całego dysku.
   - Wybranych katalogów.
   - Pojedynczych plików.
   - Plików spakowanych oraz skompresowanych.
   - Dysków sieciowych.
   - Dysków przenośnych.
8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   - Wybranych plików.
   - Wybranych procesów.
   - Wybranych lokalizacji.
   - Wybranych rozszerzeń.
9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

   A. typ urządzenia:
      - pamięci masowe,
      - optyczne pamięci masowe,

B. parametry urządzenia:
      - numer seryjny,
      - producent,
      - model.

C. typ dostępu:
      - brak możliwości zapisu,
      - pełen dostęp,
      - brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - Microsoft Windows Server 2012 R2,
   - Microsoft Windows Server 2016,
   - Microsoft Windows Server 2019,
   - Microsoft Windows Server 2022,
   - Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.
   - Adware.
   - Spyware.
   - Dialer.
   - Phishing.
   - 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 system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    - całego dysku,
    - wybranych katalogów,
    - pojedynczych plików,
    - plików spakowanych oraz skompresowanych,
    - dysków sieciowych,
    - dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
    - nazwy wykrycia,
    - sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. 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.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    A. 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.

B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. C. Raport musi posiadać co najmniej:
   - Listę zainstalowanych aplikacji,
   - Listę usług systemowych,
   - informacje o systemie operacyjnym i sprzęcie,
   - Listę aktywnych procesów i połączeń sieciowych,
   - harmonogram systemu operacyjnego,
   - Szczegóły pliku hosts,
   - Informacje o sterowników.

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
   - antywirus,
   - zapora osobista
   - sandbox,
   - antyspyware,
   - metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

    A. typ urządzenia:
    - Pamięci masowe.
    - Optyczne pamięci masowe.
    - Pamięci masowe Firewire.
    - Urządzenia do tworzenia obrazów.
    - Drukarki USB.
    - Urządzenia Bluetooth.
    - Czytniki kart inteligentnych.
    - Modemy.

- Porty LPT/COM.
- Urządzenia przenośne.

B. parametry urządzenia:

- Numer seryjny,
- Producent,
- Model.

C. typ dostępu:

- Brak możliwości zapisu,
- Pełen dostęp,
- Ostrzeżenie użytkownika,
- Brak dostępu.

18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
    - MS SQL.
    - Active Directory.
    - IIS.
    - Sysvol.
    - DNS.
    - DHCP.
    - Hyper-V.
    - Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - Skanowanie portów TCP oraz UDP,
        - Wykrywanie duplikacji adresu IP,
        - Atak zatruwania ARP,
        - Nieprawidłowa długość pakietu TCP oraz UDP.

    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        - RDP,
        - SMB,
        - My SQL,
        - MS SQL.

C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

A. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

- tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - RedHat Enterprise Linux (RHEL),
   - Rocky Linux,
   - Ubuntu,
   - Debian,
   - SUSE Linux Enterprise Server (SLES),
   - Oracle Linux,
   - Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.
   - Adware.
   - Spyware.
   - Dialer.
   - Phishing.
   - Backdoor.

3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. 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.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    - całego dysku,
    - wybranych katalogów,
    - pojedynczych plików,
    - plików spakowanych oraz skompresowanych,
    - dysków sieciowych,
    - dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    - Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

12. 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.
13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
    - proces budowania obrazu kontenera,
    - wdrażanie obrazu kontenera.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
    A. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
        - Android,
        - iOS,
        - iPadOS.
    B. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
        - Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
        - Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
        - VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
        - Apple Business Manager (ABM),
        - Android Enterprise (co najmniej w zakresie Device Owner).
3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    - usunięcie zawartości urządzenia,
    - przywrócenie urządzenia do ustawień fabrycznych,
    - zablokowanie urządzenia,
    - uruchomienie sygnału dźwiękowego,
    - lokalizację GPS,
    - Resetowanie hasła blokady ekranu.
4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

5. MDM musi umożliwiać co najmniej:

   A. Dla systemów iOS oraz iPadOS

   - konfigurację kont e-mail,
   - konfigurację połączeń VPN,
   - Konfigurację połączeń Wi-Fi,
   - Konfigurację listy certyfikatów,
   - możliwość uruchomienia trybu jednej aplikacji.

   B. Dla systemu Android:

   - blokadę wykonywania połączeń,
   - blokadę konfiguracji sieci Wi-Fi,
   - blokadę konfiguracji tuneli VPN,
   - zarządzenie aktualizacjami sytemu operacyjnego,
   - blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
   - Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
   - Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
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 zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

   A. Złożoność kodu blokady ekranu:
      - Wzór
      - PIN
      - Hasło

   B. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

   C. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   - nazwę aplikacji,
   - nazwę pakietu,
   - kategorię sklepu Google Play,

- uprawnienia aplikacji,
- pochodzenie aplikacji z nieznanego źródła.

6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Wsparcie techniczne.

- Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.