OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Oprogramowanie Sekoia Defend Prime, ESET PROTECT Elite, Safetica 11 PRO On-Prem dla Powiatowej Stacji Sanitarno – Epidemiologicznej (dalej: PSSE) w Gliwicach

1. Opis ogólny

1.1. Przedmiotem zamówienia jest dostawa uprawnień licencyjnych/subskrypcyjnych w formie elektronicznej dla trzech zintegrowanych systemów cyberbezpieczeństwa (Sekoia Defend Prime, ESET PROTECT Elite oraz Safetica 11 PRO On-Prem) wraz z ich kompleksową instalacją, konfiguracją, wdrożeniem i świadczeniem asysty technicznej w języku polskim.

1.2. Status środowiska: Żaden z zamawianych systemów nie jest obecnie użytkowany ani zainstalowany w środowisku Zamawiającego. Zamówienie dotyczy budowy nowego, zintegrowanego środowiska ochrony IT od podstaw. W związku z tym w dokumentacji nie występują wymagania dotyczące migracji archiwalnych danych ani przenoszenia starych polityk bezpieczeństwa.

2. Ogólne wymagania dostawy i licencjonowania

Wszystkie dostarczane licencje i subskrypcje muszą spełniać następujące formalno-prawne wymagania ogólne (wzorowane na standardach branżowych i instytucji badawczo-rozwojowych):

- **Kanał dystrybucji:** Wykonawca dostarczy legalne uprawnienia licencyjne/subskrypcyjne pochodzące bezpośrednio od Producentów lub z oficjalnych, autoryzowanych przez Producentów kanałów dystrybucyjnych na terenie Unii Europejskiej.
- **Forma dostawy:** Dostawa licencji nastąpi w formie elektronicznej na konto zakupowe Zamawiającego lub na wskazany adres e-mail, wraz z kompletem certyfikatów licencyjnych
  i kluczy aktywacyjnych.
- **Gwarancja aktualizacji:** Zamawiający w całym okresie trwania umowy ma zagwarantowane prawo do korzystania z najnowszych wersji oprogramowania, baz sygnatur, silników detekcyjnych, baz reputacyjnych oraz poprawek bezpieczeństwa udostępnianych przez producenta bez dodatkowych opłat.
- **Funkcjonalność równoważna lub szersza:** Zamawiający dopuszcza zaoferowanie produktów
  o parametrach technicznych lub funkcjonalności szerszej niż opisana w niniejszym OPZ, pod warunkiem pełnego spełnienia wymagań minimalnych.

- **Swoboda migracji:** Licencje nie mogą ograniczać możliwości migracji oprogramowania lub maszyn wirtualnych pomiędzy serwerami/hostami w ramach infrastruktury Zamawiającego.
- **Wsparcie techniczne:** Wykonawca zapewni pełny dostęp do oficjalnego wsparcia technicznego producentów oraz wsparcia wdrożeniowego w języku polskim przez cały okres obowiązywania subskrypcji.

2.1. Zestawienie ilościowo-czasowe zamawianych subskrypcji

System / Oprogramowanie	Typ / Architektura	Wolumen / Liczba	Okres subskrypcji
Sekoia Defend Prime	SaaS (Chmura UE) / SIEM & SOAR	165 assetów (zasobów)	36 miesięcy
ESET PROTECT Elite	SaaS / On-Prem / EDR & XDR	150 agentów / urządzeń	29 miesięcy (24 miesiące od 28.03.2027 r.)
Safetica 11 PRO On-Prem	On-Premises / DLP & Audyt	150 licencji / użytkowników	36 miesięcy

3. Wymagania podmiotowe wobec Wykonawcy (ISO 27001 i ISO 9001)

3.1. Wymagane certyfikaty: Wykonawca składający ofertę musi wykazać się posiadaniem wdrożonych i certyfikowanych systemów zarządzania ISO/IEC 27001 (Zarządzanie Bezpieczeństwem Informacji) oraz ISO 9001 (Zarządzanie Jakością) w zakresie świadczenia usług IT, dostaw oprogramowania oraz integracji systemów bezpieczeństwa.

3.2. Uzasadnienie proporcjonalności wymogu: Przedmiot zamówienia obejmuje bezpośredni dostęp do infrastruktury teleinformatycznej PSSE oraz konfigurację kluczowych systemów przetwarzających dane wrażliwe (DLP, EDR, SIEM). Posiadanie przez Wykonawcę certyfikatu ISO 27001 stanowi gwarancję zachowania poufności, integralności i procedur ochronnych podczas prac wdrożeniowych, zaś ISO 9001 zapewnia należytą jakość oraz powtarzalność procesów serwisowych.

3.3. Dopuszczenie dowodów równoważnych: Zgodnie z art. 104 i 105 ustawy Prawo Zamówień Publicznych, Zamawiający akceptuje również odpowiednie certyfikaty wydane przez jednostki wyznaczone inne równoważne środki dowodowe (np. sprawozdania z audytów niezależnych jednostek akredytowanych) potwierdzające spełnianie równoważnych wymagań w zakresie zarządzania jakością i bezpieczeństwem informacji.

4. Szczegółowe specyfikacje techniczne i funkcjonalne

4.1. Sekoia Defend Prime (SIEM / SOAR)

1. Rozwiązanie klasy SIEM / SOAR musi być dostępne z poziomu chmury producenta z miejscem przechowywania logów na terenie UE.
2. Logowanie do instancji chmurowej rozwiązania, musi umożliwiać wykorzystaniem mechanizmu 2FA.
3. Rozwiązanie musi umożliwiać tworzenie kont użytkowników z odrębnymi rolami w aplikacji.
4. Rozwiązanie musi umożliwiać utworzenie własnego typu roli użytkownika i/lub wybór jednej z domyślnej:

1) Gość
2) Analityk
3) Administrator

5. Rozwiązanie musi umożliwiać przesyłania nieograniczonej ilości zdarzeń, bez wpływu na konieczną do wykupienia licencję.
6. Rozwiązanie musi posiadać katalog minimum 200 gotowych integracji (przygotowane parsery) z źródłami zdarzeń takimi jak systemy operacyjne, aplikacje i urządzenia bezpieczeństwa.
7. Rozwiązanie musi umożliwiać utworzenie własnych parserów w przypadku braku gotowej integracji.
8. Rozwiązanie musi umożliwiać generowanie powiadomień o braku otrzymywania logów per pojedyncze źródło oraz zdefiniowany czas niedostępności logów.
9. Rozwiązanie musi posiadać możliwość dzielenia instancji głównej na podinstancje, dla których mogą być zaimplementowane inne źródła logów oraz inne reguły bezpieczeństwa wyzwalające alerty w konsoli.
10. Rozwiązanie musi umożliwiać utworzenie wielu dzierżaw w ramach, których będzie możliwe tworzenie odrębnych reguł, parserów, alertów, itp.
11. Rozwiązanie musi udostępniać możliwość instalacji przekaźnika zdarzeń w postaci gotowego kontenera dla aplikacji Docker, instalowanego lokalnie na systemie Linux.
12. Rozwiązanie musi posiadać możliwość implementacji agenta na systemy Linux, Windows oraz MacOs, który bezpośrednio będzie komunikował się z instancja chmurową oraz będzie monitorował system na którym zostanie zainstalowany.
13. Agent rozwiązanie nie może wymagać dodatkowej licencji.
14. Agent musi wspierać możliwość instalacji co najmniej na poniższych systemach:
    1. Windows 8
    2. Windows 10
    3. Windows 11
    4. Windows Server 2016
    5. Windows Server 2019

6. Windows Server 2022
7. Windows Server 2025
8. Ubuntu 14.04 i nowszy
9. Debian 8 i nowszy
10. CentOS 7 i nowszy
11. Redhat 7 i nowszy
12. macOS 13 Ventura

4.2. ESET PROTECT Elite (Endpoint Protection, EDR/XDR, MFA, Szyfrowanie)

Rozwiązanie do ochrony stacji roboczych i serwerów przed szkodliwym oprogramowaniem z wykorzystaniem narzędzia EDR/XDR.

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:

1. Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.

1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
2. 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:
    1. Google Authenticator,

2. Microsoft Authenticator,
3. Authy,
4. 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:
    1. Adresy sieciowe IP.
    2. Aktywne zagrożenia
    3. Stan funkcjonowania oraz ochrony.
    4. Wersja systemu operacyjnego.
    5. Podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    1. Wyrażenie CRON.
    2. Codziennie.
    3. Cotygodniowo.
    4. Co miesiąc.
    5. Co rok.
    6. Po wystąpieniu nowego zdarzenia.
    7. 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 umożliwiać przesyłanie danych do przynajmniej dwóch różnych serwerów syslog, bez potrzeby korzystania z oprogramowania firm trzecich do dystrybucji logów.
19. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
    1. JSON.
    2. LEEF.
    3. 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:

1. Wirus. T
2. Trojan.
3. Robak.
4. Adware.
5. Spyware.
6. Dialer.
7. Phishing.
8. 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 funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
8. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
   - Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
   - Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym I zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
   - Technologia ta musi umożliwiać manualne przywracanie plików przez administratora z konsoli centralnego zarządzania.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. 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.
11. 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).

12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. 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.
14. 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).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. 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.
17. 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.

18. 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.
19. 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.

20. 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.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem system operacyjnego.
22. 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.
23. 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,
    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. 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.

25. 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.
26. 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 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 system 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.

   2.1. Adware.
   2.2. Spyware.
   2.3. Dialer.
   2.4. Phishing.
   2.5. 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.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - Microsoft Windows 10 oraz 11,
   - Microsoft Windows Server,
   - macOS 11 (Big Sur) oraz nowszych
   - RedHat Enterprise Linux (RHEL),
   - Rocky Linux,
   - Ubuntu,
   - Debian,
   - SUSE Linux Enterprise Server (SLES),
   - Oracle Linux,
   - Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-dni.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
   - archiwa,
   - skrypty,
   - pliki wykonywalne,
   - pliki rejestru systemowego (.reg),
   - możliwy spam,
   - dokumenty.

7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
   - natychmiast po ich przeanalizowaniu,
   - po upływie 30 dni,
   - nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
    - Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
    - czysty,
    - podejrzany,
    - bardzo podejrzany,
    - szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:

A. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
   - przeglądarki internetowe,
   - programy poczty e-mail,
   - nośniki wymienne,
   - pliki wyodrębnione z archiwum.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
   - Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
   - Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
   - Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
   - Hasło odzyskiwania nie może być krótsze niż 8 znaków.
   - Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.
12. Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty:
   - Microsoft Exchange 2010 SP3,
   - Microsoft Exchange 2013,
   - Microsoft Exchange 2016,
   - Microsoft Exchange 2019.
2. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról
   - Mailbox,
   - Edge,
   - Hub.
3. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange

4. Wszystkie komponenty rozwiązania ochrony serwera pocztowego Exchange muszą pracować na tym samym serwerze, na którym zainstalowany jest Microsoft Exchange (Rozwiązanie nie może pracować jako rozwiązanie typu gateway).
5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
6. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange).
7. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
8. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
   A. Rozwiązanie musi posiadać co najmniej następujące warunki:
      - nadawca,
      - odbiorca,
      - temacie wiadomości,
      - adres IP nadawcy,
      - nazwa, rozmiar i typ załącznika,
      - rozmiar wiadomości,
      - nagłówek wiadomości,
      - godzina odbioru,
      - obecność załącznika chronionego hasłem,
      - wynik SPF, DKIM i DMARC.
   B. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
      - poddaj wiadomość kwarantannie,
      - odrzuć wiadomość,
      - porzuć wiadomość w trybie dyskretnym,
      - usuń załącznik,
      - dodaj prefix tematu,
      - wyślij powiadomienie e-mail,
      - pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
9. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
10. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
11. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
12. Rozwiązanie musi posiadać mechanizm greylisting (szara lista).

13. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM.

Ochrona usług chmurowych

1. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:
   - konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),
   - konsola centralnego zarządzania musi być dostępna z poziomu interfejsu WWW,
   - konsola centralnego zarządzania musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
   - Konsola centralnego zarządzania musi być dostępne co najmniej w języku polskim oraz angielskim.
2. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług:
   - Microsoft Exchange Online.
   - Microsoft OneDrive.
   - Microsoft Sharepoint.
   - Microsoft Teams.
   - Google Workspace, w tym co najmniej Gmail i Google Drive.
3. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
4. Rozwiązanie musi umożliwiać:
   - Wybór ręczny kont użytkowników, które będą objęte ochroną,
   - Wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione.
5. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:
   - kont użytkowników, otrzymujących najwięcej spamu,
   - kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
   - kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
   - kont użytkowników, które mogę być podejrzane.
6. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty.
7. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.

A. Rozwiązanie musi posiadać co najmniej następujące warunki:
   - nadawca,
   - temacie wiadomości,
   - adres IP nadawcy,
   - nazwa, rozszerzenie i typ załącznika,
   - nagłówek wiadomości,

- godzina odbioru,
- wynik SPF, DKIM, DMARC i ARC.

B. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
- poddaj wiadomość kwarantannie,
- usuń wiadomość,
- usuń załącznik,
- dodaj prefix tematu,
- wyślij powiadomienie e-mail,
- pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.

8. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej
- w formie oryginalnego pliku,
- w formie pliku zabezpieczonego hasłem.

9. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:
- całego tenantu,
- grupy,
- grupy Teams,
- lokacji Sharepoint,
- Pojedynczego użytkownika.

10. Rozwiązanie musi korzystać z chmury reputacji plików, pochodzącego od tego samego producenta rozwiązania antywirusowego:
- możliwość automatycznego wysłania sumy kontrolnej
- możliwość automatycznego wysłania fragmentu pliku.

11. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:
- brak czynności.
- przenieś do spamu.
- poddaj wiadomość kwarantannie.
- poddaj załącznik kwarantannie.
- przenieś do kosza.
- usuń załącznik.
- zastąp załącznik.
- usuń wiadomość.

12. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako:
- SPAM.
- Phishing.

13. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
    - Archiwa.
    - Skrypty.
    - Pliki wykonywalne.
    - Pliki rejestru systemowego (.reg).
    - Możliwy spam.
    - Dokumenty.
14. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
    - natychmiast po ich przeanalizowaniu,
    - po upływie 30 dni,
    - nigdy.
15. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.

A. Powiadomienia muszą dotyczyć wykryć co najmniej:
    - zagrożeń w wiadomościach,
    - phishing w wiadomościach,
    - zagrożeń w plikach onedrive,
    - zagrożeń na dysku Google Drive,

B. Powiadomienia muszą być możliwe do wysłania w co najmniej jednym z następujących języków:
    - Język polski,
    - Język angielski.

Vulnerability Assessment and Patch Management

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie musi mieć możliwości wykrywania podatności:

A. w tym co najmniej następujących systemach operacyjnych:
    - Windows,
    - macOS,
    - Linux

B. w aplikacjach zainstalowanych na zarządzanych stacjach.

3. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE.
4. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych. Zarządzanie musi się odbywać z poziomu tej samej konsoli co rozwiązanie antywirusowe, pochodzące od tego samego producenta.

5. Rozwiązanie musi umożliwiać utworzenie haromonogramu automatycznego wykrywania podatności.
6. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:
   - nazwę aplikacji lub systemu operacyjnego
   - punktacje CVSS
   - opis wykrytej podatności
   - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
7. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach.
8. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji.
9. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.
   - Automatyczne aktualizacje będą aplikowane tylko dla wskazanych aplikacji w białej liście.
   - Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.
    - Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich – ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.
    - Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
11. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
12. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
13. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności.

Two-factor authentication / multi-factor authentication

1. Rozwiązanie musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi pozwalać na instalację oprogramowania na co najmniej następujących systemach operacyjnych:

A. Systemy serwerowe:
   - Microsoft Windows Server 2012 R2,
   - Microsoft Windows Server 2016,

- Microsoft Windows Server 2019,
- Microsoft Windows Server 2022,
- Microsoft Windows Server 2025.

B. Systemy kliencie:

- Windows 10,
- Windows 11.

5. Rozwiązanie musi posiadać integrację z następującymi rozwiązaniami:
   - Microsoft Exchange,
   - Microsoft Dynamics CRM,
   - Microsoft Sharepoint,
   - Microsoft Remote Desktop Web Access,
   - Microsoft Terminal Services Web Access,
   - Microsoft Remote Web Access,
   - Active Directory Federation Services.
6. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników podczas logowania do co najmniej:
   - klienta VPN,
   - systemu macOS
   - systemu Linux,
   - połączenia SSH.
7. Rozwiązanie musi oferować dedykowaną bezpłatną aplikację mobilną pochodzącą od tego samego producenta rozwiązania 2FA/MFA.

A. Aplikacja mobilna musi wspierać następujące systemy:

- Android,
- iOS.

B. Aplikacja mobilna musi umożliwiać uwierzytelnienie użytkownika przy pomocy co najmniej:

- Generowanego kodu OTP w tym co najmniej HOTP i TOTP.
- Powiadomienia PUSH.
- Aplikacja mobilna musi posiadać możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.
- Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP musi odbywać się w trybie offline.
- Aplikacja musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.

8. Rozwiązanie musi oferować alternatywne możliwości uwierzytelnienie użytkownika w tym co najmniej:

- OTP dostarczonego przy pomocy wiadomości SMS,
- OTP dostarczonego przy pomocy wiadomości e-mail,
- tokenu sprzętowego,
- FIDO,
- klucza odzyskiwania (MRK).

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
   - Tworzenie procesów.
   - Uruchamianie, zatrzymanie i modyfikacja usług.
   - Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym.
   - Usuwanie oraz zmiana nazw plików.
   - Tworzenie i usuwanie kluczy rejestru systemowego.
   - Ładowanie bibliotek DLL.
   - Zalogowanie użytkowników.

   A. elementy sieciowe, w tym co najmniej:
   - Pobranie plików wykonywalnych.
   - Zestawienie połączeń TCP/IP.
   - Zapytania http.
   - Zapytania DNS.
4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

   A. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
   - Blokowanie pliku wykonywalnego.
   - Blokowanie pliku wykonywalnego i poddanie go kwarantannie.
   - Blokowanie podejrzanej biblioteki DLL.
   - Zakończenie procesu.
   - Skanowanie komputera w poszukiwaniu zagrożeń.
   - Wyłączenie komputera.
   - Izolacja sieciowa hosta dla systemów Windows oraz Linux.

- Wylogowanie użytkownika.

B. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

A. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

- Proces.
- Proces nadrzędny (proces rodzica).
- Nazwę procesu.
- Ścieżkę procesu.
- Wiersz polecenia.
- Wydawcę.
- Typ podpisu cyfrowego.
- SHA-1.
- SHA-2.
- Użytkownika.

C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.

6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

A. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.

B. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):

- SHA-1.
- SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:

- Hash pliku SHA-1.
- Hash pliku SHA-256.
- Hash pliku MD5.
- Typ sygnatury podpisu cyfrowego.
- Wydawcę certyfikatu.
- Wersję pliku.
- Oryginalną nazwę pliku.
- Rozmiar pliku.

- Reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego.
- Pierwsze uruchomienie pliku w środowisku.
- Ostatnie uruchomienie pliku w środowisku.

8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
   - Oznaczania ich jako bezpieczne lub niebezpieczne.
   - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
   - Zablokowania wykonywania i wykorzystania pliku.
   - Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
   - Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
   - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
   - Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
   - Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
   - Administrator musi posiadać możliwość odczytania informacji o języku skryptu.
10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
    - Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
13. Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR, przynajmniej w oparciu o:
    - Wyszukiwanie dowolnego tekstu.
    - Wyszukiwanie, pozwalające łączyć ze sobą różne słowa, oddalone od siebie nie więcej niż 3 innymi słowami.
    - Wyszukiwanie po nazwie procesów.
    - Wyszukiwanie po ocenie ryzyka.
    - Filtrowanie według daty.

Ochrona serwerów w chmurze AWS, Microsoft Azure i Google Cloud Platform

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie musi udostępniać możliwość integracji przynajmniej z rozwiązaniami:
   - Microsoft Azure.
   - Google Cloud Platform.
   - Amazon Web Services.
3. Rozwiązanie powinno zapewniać możliwość zarówno automatycznego uruchamiania ochrony dla nowych i już istniejących maszyn wirtualnych, jak i ręcznego wskazania wybranych zasobów do objęcia ochroną.

Wsparcie techniczne.

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

4.3. Safetica 11 PRO On-Prem (Data Loss Prevention)

1. System operacyjny:
   a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   c. Windows Server 2019 lub nowszy
   d. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach:
   a. Windows Server 2019 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
   a. MS SQL Server 2016 SP1 CU2 lub nowsze,
   b. MS SQL Server 2016 SP1 CU2 Express,
   c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalną klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli dostępnej z poziomu przeglądarki internetowej.

11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość utworzenia i usuwania kont administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu.
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi mieć możliwość wymuszenia synchronizacji ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP.
18. Administrator musi mieć możliwość dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa w skonfigurowanym powiadomieniu.
19. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o co najmniej poniższe czynności:
    a. uruchomione aplikacje,
    b. podłączone urządzenia,
    c. odwiedzane strony internetowe,
    d. wydrukowane dokumenty,
    e. wysyłane wiadomości e-mail,
    f. odebrane wiadomości e-mail,
    g. czynności na plikach.

5. Zakres usług wdrożeniowych i asysty technicznej

W ramach zaoferowanej ceny ryczałtowej Wykonawca zobowiązany jest do kompleksowej realizacji następujących prac wdrożeniowych:

- **1. Dostawa licencji:** Przekazanie oficjalnych elektronicznych certyfikatów licencyjnych, kluczy aktywacyjnych oraz dostępów do kont zakupowych.
- **2. Instalacja i konfiguracja:** Instalacja serwera Safetica ON-PREM na zasobach wirtualnych przygotowanych przez Zamawiającego, uruchomienie przekaźnika Docker dla Sekoia Defend oraz konfiguracja instancji SaaS dla Sekoia i ESET.
- **3. Wdrożenie agentów i polityk:** Instalacja agentów oprogramowania na stacjach roboczych i serwerach Stacji, zdefiniowanie reguł klasyfikacji DLP, reguł EDR oraz parserów i reguł detekcji w SIEM.
- **4. Integracja systemów:** Skonfigurowanie płynnego przesyłania zdarzeń i alertów z systemów ESET i Safetica do platformy Sekoia Defend (SIEM/SOAR).

- **5. Szkolenie administratorów:** Przeprowadzenie warsztatu/instruktażu dla administratorów Zamawiającego w zakresie zarządzania konsolami, analizy incydentów i modyfikacji polityk.
- **6. Wsparcie i serwis:** Świadczenie bezpłatnej asysty technicznej i poprawek w języku polskim przez okres 36 miesięcy od podpisania protokołu odbioru.

6. Procedura odbioru zamówienia i testy współdziałania

6.1. Warunki odbioru: Odbiór zamówienia nastąpi po zakończeniu prac instalacyjnych, weryfikacji poprawności wygenerowanych licencji oraz przeprowadzeniu obowiązkowych testów końcowych.

6.2. Testy współdziałania: Przed podpisaniem protokołu odbioru Wykonawca w obecności przedstawicieli Zamawiającego przeprowadzi testy potwierdzające: (a) poprawną komunikację i przesyłanie zdarzeń z ESET i Safetica do Sekoia Defend, (b) brak konfliktów wydajnościowych agentów na stacjach roboczych, (c) prawidłowe wyzwalanie alertów DLP i EDR na próbach testowych.

6.3. Protokół odbioru: Pozytywny wynik testów oraz przekazanie kompletnej dokumentacji powdrożeniowej stanowi podstawę do podpisania jednego, końcowego protokołu odbioru jakościowego i ilościowego.

Potwierdzam zgodność kopii z dokumentem elektronicznym:

Identyfikator dokumentu	964cc8a42c8a4049a87cd4b873f0bbbd	
Nazwa dokumentu	zal-01-do-SWZ-OPZ.docx	
Tytuł dokumentu	zal-01-do-SWZ-OPZ	
Skrót dokumentu	9f7667a038b0bb5c784ec378dd284bfefcdf933d9f1dcb0a14988e873fd1288d	
Wersja dokumentu	1.0	
Data dokumentu	2026-10-30	
Akceptacja	Zaakceptowany przez	Marcin Ciuk (INF) Starszy informatyk
	Data akceptacji	2026-10-30
	Wersja dokumentu akceptacji	1.0
	EZD RP 26.401.9	
Data wydruku	2026-10-30	
Autor wydruku	Manuela Rzeźwicka (Starszy specjalista) OK	