**Dotyczy postępowania: Dostawa oprogramowania/licencji klasy XDR dla potrzeb „MCZ” S.A.**

**Opis Przedmiotu Zamówienia**

**Wykonawca: ……………………………………………**

**Nazwa i typ oprogramowania: ……………………………………………**

**Producent/ Kraj: ……………………………………………**

\*Odpowiedź NIE w przypadku parametrów wymaganych powoduje odrzucenie oferty

| **L. p.** | **Wymagane parametry** | **Parametr wymagany** | **Parametr oceniany** | **Potwierdzenie spełnienia parametru wymaganego / opis oferowanego rozwiązania**  należy wprowadzić opis oferowanego rozwiązania |
| --- | --- | --- | --- | --- |
|  | 1. Dostawa oprogramowania/licencji dla 850 stanowisk na okres od 05.03.2026r. do 30.06.2029r. | Tak, podać | Bez oceny |  |
|  | 1. **Administracja zdalna** |  |  |  |
|  | 1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu www. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej: 2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania, 3. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta, 4. Buforowanie ruchu HTTPS. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.    1. Uwierzytelnianie dwuskładnikowe musi być realizowane 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.    1. 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. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim    1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwość tagowania obiektów. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.    1. Eksport danych musi być możliwy w co najmniej następujących formatach:       1. JSON,       2. LEEF,       3. CEF. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona stacji roboczych - Windows** |  |  |  |
|  | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:    1. wirus,    2. trojan,    3. robak,    4. adware,    5. spyware,    6. dialer,    7. phishing,    8. backdoor. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.    1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.    2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).    3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:    1. całego dysku,    2. wybranych katalogów,    3. pojedynczych plików,    4. plików spakowanych oraz skompresowanych,    5. dysków sieciowych,    6. dysków przenośnych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:    1. wybranych plików,    2. wybranych procesów,    3. wybranych lokalizacji,    4. wybranych rozszerzeń,    5. nazwy wykrycia,    6. sumy kontrolnej (SHA1). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi integrować się z Intel Threat Detection Technology. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:    1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.    2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.    3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:    1. typ urządzenia:       1. pamięci masowe,       2. optyczne pamięci masowe,       3. pamięci masowe Firewire,       4. urządzenia do tworzenia obrazów,       5. drukarki USB,       6. urządzenia Bluetooth,       7. czytniki kart inteligentnych,       8. modemy,       9. porty LPT/COM,       10. urządzenia przenośne.    2. parametry urządzenia:       1. numer seryjny,       2. producent,       3. model.    3. typ dostępu:       1. brak możliwości zapisu,       2. pełen dostęp,       3. ostrzeżenie użytkownika,       4. brak dostępu. | Tak, podać | Bez oceny |  |
|  | 1. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,    2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,    3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,    4. 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,    5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.    1. 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.    2. 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.    3. Raport musi posiadać co najmniej:       1. Listę zainstalowanych aplikacji,       2. Listę usług systemowych,       3. Informacje o systemie operacyjnym i sprzęcie,       4. Listę aktywnych procesów i połączeń sieciowych,       5. Harmonogram systemu operacyjnego,       6. Szczegóły pliku hosts,       7. Informacje o sterownikach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu    1. antywirus,    2. zapora osobista    3. sandbox,    4. antyspyware,    5. metody heurystyczne. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.    1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.    2. Ochrona musi być realizowana w oparciu o co najmniej:       1. globalna czarna lista RBL,       2. czarna lista użytkownika,       3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:    1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:       1. Skanowanie portów TCP oraz UDP,       2. Wykrywanie duplikacji adresu IP,       3. Atak zatruwania ARP,       4. Nieprawidłowa długość pakietu TCP oraz UDP.    2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:       1. RDP,       2. SMB,       3. My SQL,       4. MS SQL.    3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.    1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.    2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:       1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,       2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,       3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,       4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.          1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.    1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.    2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.    3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.    1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.    2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:       1. Treść komunikatu,       2. Obraz. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona stacji roboczych – MacOS** |  |  |  |
|  | 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:    1. wirus,    2. trojan,    3. robak,    4. adware,    5. spyware,    6. dialer,    7. phishing,    8. backdoor. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych I wykonywanych plików. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi chronić pliki co najmniej za pomocą:    1. Sygnatur wirusów.    2. Reputacji chmurowej. | Tak, podać | Bez oceny |  |
|  | 1. 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). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:    1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.    2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.    3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. |  |  |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:    1. całego dysku,    2. wybranych katalogów,    3. pojedynczych plików,    4. plików spakowanych oraz skompresowanych,    5. Dysków sieciowych,    6. dysków przenośnych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:    1. wybranych plików,    2. wybranych procesów,    3. wybranych lokalizacji,    4. wybranych rozszerzeń,    5. nazwy wykrycia,    6. sumy kontrolnej (SHA1). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.    1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.    2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:       1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,       2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący, | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona stacji roboczych – Linux** |  |  |  |
|  | 1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:    1. Ubuntu Desktop,    2. Red Hat Enterprise Linux    3. Linux Mint. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:    1. Cinnamon,    2. GNOME,    3. KDE,    4. MATE,    5. XFCE. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:    1. wirus,    2. trojan,    3. robak,    4. adware,    5. spyware,    6. dialer,    7. phishing,    8. backdoor. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:    1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.    2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:    1. całego dysku,    2. wybranych katalogów,    3. pojedynczych plików,    4. plików spakowanych oraz skompresowanych,    5. dysków sieciowych,    6. dysków przenośnych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:    1. wybranych plików,    2. wybranych procesów,    3. wybranych lokalizacji,    4. wybranych rozszerzeń, | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:    1. typ urządzenia:       1. pamięci masowe,       2. optyczne pamięci masowe,    2. parametry urządzenia:       1. numer seryjny,       2. producent,       3. model.    3. typ dostępu:       1. brak możliwości zapisu,       2. pełen dostęp,       3. brak dostępu. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona serwera – Windows Server** |  |  |  |
|  | 1. Rozwiązanie musi wspierać systemy w tym co najmniej:    1. Microsoft Windows Server 2012 R2,    2. Microsoft Windows Server 2016,    3. Microsoft Windows Server 2019,    4. Microsoft Windows Server 2022,    5. Microsoft Windows Server 2025. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:    1. wirus,    2. trojan,    3. robak,    4. adware,    5. spyware,    6. dialer,    7. phishing,    8. backdoor. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. | Tak, podać | Bez oceny |  |
|  | 1. 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 | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:    1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.    2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.    3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:    1. całego dysku,    2. wybranych katalogów,    3. pojedynczych plików,    4. plików spakowanych oraz skompresowanych,    5. dysków sieciowych,    6. dysków przenośnych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:    1. wybranych plików,    2. wybranych procesów,    3. wybranych lokalizacji,    4. wybranych rozszerzeń,    5. nazwy wykrycia,    6. sumy kontrolnej (SHA1). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. | Tak, podać | Bez oceny |  |
|  | 1. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,    2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,    3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,    4. 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,    5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.    1. 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.    2. 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    3. Raport musi posiadać co najmniej:       1. Listę zainstalowanych aplikacji       2. Listę usług systemowych       3. informacje o systemie operacyjnym i sprzęcie,       4. Listę aktywnych procesów i połączeń sieciowych,       5. harmonogram systemu operacyjnego,       6. Szczegóły pliku hosts       7. Informacje o sterowników | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu    1. antywirus,    2. zapora osobista    3. sandbox,    4. antyspyware,    5. metody heurystyczne. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi skanować system wirtualny w trybie online oraz ofline w środowisku Hyper-V. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:    1. typ urządzenia:       1. pamięci masowe,       2. optyczne pamięci masowe,       3. pamięci masowe Firewire,       4. urządzenia do tworzenia obrazów,       5. drukarki USB,       6. urządzenia Bluetooth,       7. czytniki kart inteligentnych,       8. modemy,       9. porty LPT/COM,       10. urządzenia przenośne.    2. parametry urządzenia:       1. numer seryjny,       2. producent,       3. model.    3. typ dostępu:       1. brak możliwości zapisu,       2. pełen dostęp,       3. ostrzeżenie użytkownika,       4. brak dostępu. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:    1. MS SQL,    2. Active Directory,    3. IIS,    4. Sysvol,    5. DNS,    6. DHCP,    7. Hyper-V,    8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:    1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:       1. Skanowanie portów TCP oraz UDP,       2. Wykrywanie duplikacji adresu IP,       3. Atak zatruwania ARP,       4. Nieprawidłowa długość pakietu TCP oraz UDP.    2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:       1. RDP,       2. SMB,       3. My SQL,       4. MS SQL.    3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.    1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:       1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,       2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,       3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,       4. ryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.   21.1.4.1 Administrator musi posiadać możliwość skonfigurowania czasu działania trybu. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona serwera – Linux** |  |  |  |
|  | 1. Rozwiązanie musi wspierać systemy w tym co najmniej:    1. RedHat Enterprise Linux (RHEL),    2. Rocky Linux,    3. Ubuntu,    4. Debian,    5. SUSE Linux Enterprise Server (SLES),    6. Oracle Linux,    7. Amazon Linux. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:    1. wirus,    2. trojan,    3. robak,    4. adware,    5. spyware,    6. dialer,    7. phishing,    8. backdoor. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:    1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.    2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:    1. całego dysku,    2. wybranych katalogów,    3. pojedynczych plików,    4. plików spakowanych oraz skompresowanych,    5. dysków sieciowych,    6. dysków przenośnych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:    1. wybranych plików,    2. wybranych procesów,    3. wybranych lokalizacji,    4. wybranych rozszerzeń, | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.    1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:    1. proces budowania obrazu kontenera,    2. wdrażanie obrazu kontenera. | Tak, podać | Bez oceny |  |
|  | 1. **Mobile Device Management** |  |  |  |
|  | 1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. | Tak, podać | Bez oceny |  |
|  | 1. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.    1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:       1. Android,       2. iOS,       3. iPadOS.    2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:       1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),       2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),       3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),       4. Apple Business Manager (ABM),       5. Android Enterprise (co najmniej w zakresie Device Owner). | Tak, podać | Bez oceny |  |
|  | 1. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:    1. usunięcie zawartości urządzenia,    2. przywrócenie urządzenia do ustawień fabrycznych,    3. zablokowanie urządzenia,    4. uruchomienie sygnału dźwiękowego,    5. lokalizację GPS,    6. Resetowanie hasła blokady ekranu. | Tak, podać | Bez oceny |  |
|  | 1. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. | Tak, podać | Bez oceny |  |
|  | 1. MDM musi umożliwiać co najmniej:    1. Dla systemów iOS oraz iPadOS       1. konfigurację kont e-mail,       2. konfigurację połączeń VPN,       3. Konfigurację połączeń Wi-Fi,       4. Konfigurację listy certyfikatów,       5. możliwość uruchomienia trybu jednej aplikacji.    2. Dla systemu Android:       1. blokadę wykonywania połączeń,       2. blokadę konfiguracji sieci Wi-Fi,       3. blokadę konfiguracji tuneli VPN,       4. zarządzenie aktualizacjami sytemu operacyjnego,       5. blokadę zmiany tapety urządzenia. | Tak, podać | Bez oceny |  |
|  | 1. **Mobile Threat Defense (MTD) dla systemu Android** |  |  |  |
|  | 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:    1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.    2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:    1. Złożoność kodu blokady ekranu:       1. Wzór,       2. PIN,       3. Hasło,    2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,    3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:    1. nazwę aplikacji,    2. nazwę pakietu,    3. kategorię sklepu Google Play,    4. uprawnienia aplikacji,    5. pochodzenie aplikacji z nieznanego źródła. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing. | Tak, podać | Bez oceny |  |
|  | 1. **Sandbox w chmurze** |  |  |  |
|  | 1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać systemy w tym co najmniej:    1. Microsoft Windows 10 oraz 11,    2. Microsoft Windows Server,    3. macOS 11 (Big Sur) oraz nowszych    4. RedHat Enterprise Linux (RHEL),    5. Rocky Linux,    6. Ubuntu,    7. Debian,    8. SUSE Linux Enterprise Server (SLES),    9. Oracle Linux,    10. Amazon Linux. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:    1. archiwa,    2. skrypty,    3. pliki wykonywalne,    4. pliki rejestru systemowego (.reg),    5. możliwy spam,    6. dokumenty. | Tak, podać | Bez oceny |  |
|  | 1. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:    1. natychmiast po ich przeanalizowaniu,    2. po upływie 30 dni,    3. nigdy. | Tak, podać | Bez oceny |  |
|  | 1. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. | Tak, podać | Bez oceny |  |
|  | 1. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.    1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane. | Tak, podać | Bez oceny |  |
|  | 1. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:    1. czysty,    2. podejrzany,    3. bardzo podejrzany,    4. szkodliwy. | Tak, podać | Bez oceny |  |
|  | 1. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:    1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:       1. przeglądarki internetowe,       2. programy poczty e-mail,       3. nośniki wymienne,       4. pliki wyodrębnione z archiwum. | Tak, podać | Bez oceny |  |
|  | 1. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. **Szyfrowanie** |  |  |  |
|  | 1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.    1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.    2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania. | Tak, podać | Bez oceny |  |
|  | 1. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.    1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.    2. Hasło odzyskiwania nie może być krótsze niż 8 znaków.    3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0. | Tak, podać | Bez oceny |  |
|  | 1. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku. | Tak, podać | Bez oceny |  |
|  | 1. **Endpoint Detection and Response / eXtended Detection and Response** |  |  |  |
|  | 1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:    1. tworzenie procesów,    2. uruchamianie, zatrzymanie i modyfikacja usług,    3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,    4. usuwanie oraz zmiana nazw plików,    5. tworzenie i usuwanie kluczy rejestru systemowego,    6. ładowanie bibliotek DLL,    7. zalogowanie użytkowników,    8. elementy sieciowe, w tym co najmniej       1. pobranie plików wykonywalnych,       2. zestawienie połączeń TCP/IP,       3. zapytania HTTP,       4. zapytania DNS. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.    1. 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:       1. blokowanie pliku wykonywalnego,       2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,       3. blokowanie podejrzanej biblioteki DLL,       4. zakończenie procesu,       5. skanowanie komputera w poszukiwaniu zagrożeń,       6. wyłączenie komputera,       7. izolacja sieciowa hosta,       8. wylogowanie użytkownika.    2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.    1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.    2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:       1. proces,       2. proces nadrzędny (proces rodzica),       3. nazwę procesu,       4. ścieżkę procesu,       5. wiersz polecenia,       6. wydawcę,       7. typ podpisu,       8. SHA-1,       9. SHA-2,       10. użytkownika.    3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.    1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.    2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):       1. SHA-1,       2. SHA-256. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:    1. hash pliku SHA-1,    2. hash pliku SHA-256,    3. hash pliku MD5,    4. typ sygnatury podpisu cyfrowego,    5. wydawcę certyfikatu,    6. wersję pliku,    7. oryginalną nazwę pliku,    8. rozmiar pliku,    9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,    10. pierwsze uruchomienie pliku w środowisku,    11. ostatnie uruchomienie pliku w środowisku, | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:    1. oznaczania ich jako bezpieczne lub niebezpieczne,    2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,    3. zablokowania wykonywania i wykorzystania pliku,    4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).    1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.    2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,    3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.    4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.    1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona serwera pocztowego MS Exchange** |  |  |  |
|  | 1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty:    1. Microsoft Exchange 2010 SP3,    2. Microsoft Exchange 2013,    3. Microsoft Exchange 2016,    4. Microsoft Exchange 2019. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról    1. Mailbox,    2. Edge,    3. Hub. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange | Tak, podać | Bez oceny |  |
|  | 1. 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). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.    1. Rozwiązanie musi posiadać co najmniej następujące warunki:       1. nadawca,       2. odbiorca,       3. temacie wiadomości,       4. adres IP nadawcy,       5. nazwa, rozmiar i typ załącznika,       6. rozmiar wiadomości,       7. nagłówek wiadomości,       8. godzina odbioru,       9. obecność załącznika chronionego hasłem,       10. wynik SPF, DKIM i DMARC.    2. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:       1. poddaj wiadomość kwarantannie,       2. odrzuć wiadomość,       3. porzuć wiadomość w trybie dyskretnym,       4. usuń załącznik,       5. dodaj prefix tematu,       6. wyślij powiadomienie e-mail,       7. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty. | Tak, podać | Bez oceny |  |
|  | 1. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty. | Tak, podać | Bez oceny |  |
|  | 1. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać mechanizm greylisting (szara lista). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM. | Tak, podać | Bez oceny |  |
|  | 1. **Ochrona usług chmurowych** |  |  |  |
|  | 1. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:    1. konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),    2. konsola centralnego zarządzania musi być dostępna z poziomu interfejsu WWW,    3. konsola centralnego zarządzania musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.    4. Konsola centralnego zarządzania musi być dostępne co najmniej w języku polskim oraz angielskim. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług:    1. Microsoft Exchange Online,    2. Microsoft OneDrive,    3. Microsoft Sharepoint,    4. Microsoft Teams,    5. Google Workspace, w tym co najmniej       1. Gmail,       2. Google Drive. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać:    1. Wybór ręczny kont użytkowników, które będą objęte ochroną,    2. Wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:    1. kont użytkowników, otrzymujących najwięcej spamu,    2. kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,    3. kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,    4. kont użytkowników, które mogę być podejrzane. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.    1. Rozwiązanie musi posiadać co najmniej następujące warunki:       1. nadawca,       2. temacie wiadomości,       3. adres IP nadawcy,       4. nazwa, rozszerzenie i typ załącznika,       5. nagłówek wiadomości,       6. godzina odbioru,       7. wynik SPF, DKIM, DMARC i ARC.    2. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:       1. poddaj wiadomość kwarantannie,       2. usuń wiadomość,       3. usuń załącznik,       4. dodaj prefix tematu,       5. wyślij powiadomienie e-mail,       6. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej:    1. w formie oryginalnego pliku,    2. w formie pliku zabezpieczonego hasłem. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:    1. całego tenantu,    2. grupy,    3. grupy Teams,    4. lokacji Sharepoint,    5. Pojedynczego użytkownika. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi korzystać z chmury reputacji plików, pochodzącego od tego samego producenta rozwiązania antywirusowego:    1. możliwość automatycznego wysłania sumy kontrolnej    2. możliwość automatycznego wysłania fragmentu pliku. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:    1. brak czynności,    2. przenieś do spamu,    3. poddaj wiadomość kwarantannie,    4. poddaj załącznik kwarantannie,    5. przenieś do kosza,    6. usuń załącznik,    7. zastąp załącznik    8. usuń wiadomość. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako:    1. SPAM,    2. phishing. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:    1. archiwa,    2. skrypty,    3. pliki wykonywalne,    4. pliki rejestru systemowego (.reg),    5. możliwy spam,    6. Dokumenty. | Tak, podać | Bez oceny |  |
|  | 1. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:    1. natychmiast po ich przeanalizowaniu,    2. po upływie 30 dni,    3. nigdy. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.    1. Powiadomienia muszą dotyczyć wykryć co najmniej:       1. zagrożeń w wiadomościach,       2. phishing w wiadomościach,       3. zagrożeń w plikach onedrive,       4. zagrożeń na dysku Google Drive,    2. Powiadomienia muszą być możliwe do wysłania w co najmniej jednym z następujących języków:       1. Język polski,       2. Język angielski. | Tak, podać | Bez oceny |  |
|  | 1. **Vulnerability Assessment and Patch Management** |  |  |  |
|  | 1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi mieć możliwości wykrywania podatności:    1. w tym co najmniej następujących systemach operacyjnych:       1. Windows,       2. macOS,       3. Linux    2. w aplikacjach zainstalowanych na zarządzanych stacjach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE. | Tak, podać | Bez oceny |  |
|  | 1. 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. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać utworzenie haromonogramu automatycznego wykrywania podatności. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:    1. nazwę aplikacji lub systemu operacyjnego    2. punktacje CVSS    3. opis wykrytej podatności    4. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.    1. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście.    2. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.    1. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.    2. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności. | Tak, podać | Bez oceny |  |
|  | 1. **Two-factor authentication / Multi-factor authentication** |  |  |  |
|  | 1. Rozwiązanie musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS). | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu www. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi pozwalać na instalację oprogramowania na co najmniej następujących systemach operacyjnych:    1. Systemy serwerowe:       1. Microsoft Windows Server 2012 R2,       2. Microsoft Windows Server 2016,       3. Microsoft Windows Server 2019,       4. Microsoft Windows Server 2022,       5. Microsoft Windows Server 2025.    2. Systemy kliencie:       1. Windows 8.1,       2. Windows 10,       3. Windows 11. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać integrację z następującymi rozwiązaniami:    1. Microsoft Exchange,    2. Microsoft Dynamics CRM,    3. Microsoft Sharepoint,    4. Microsoft Remote Desktop Web Access,    5. Microsoft Terminal Services Web Access,    6. Microsoft Remote Web Access,    7. Active Directory Federation Services. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników podczas logowania do co najmniej:    1. klienta VPN,    2. systemu macOS    3. systemu Linux,    4. połączenia SSH. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi oferować dedykowaną bezpłatną aplikację mobilną pochodzącą od tego samego producenta rozwiązania 2FA/MFA.    1. Aplikacja mobilna musi wspierać następujące systemy:       1. Android,       2. iOS.    2. Aplikacja mobilna musi umożliwiać uwierzytelnienie użytkownika przy pomocy co najmniej:       1. Generowanego kodu OTP w tym co najmniej:          1. HOTP,          2. TOTP.       2. Powiadomienia PUSH.    3. Aplikacja mobilna musi posiadać możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.    4. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP musi odbywać się w trybie ofline.    5. Aplikacja musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego. | Tak, podać | Bez oceny |  |
|  | 1. Rozwiązanie musi oferować alternatywne możliwości uwierzytelnienie użytkownika w tym co najmniej:    1. OTP dostarczonego przy pomocy wiadomości SMS,    2. OTP dostarczonego przy pomocy wiadomości e-mail,    3. tokenu sprzętowego,    4. FIDO,    5. klucza odzyskiwania (MRK). | Tak, podać | Bez oceny |  |
|  | 1. **Wdrożenie, szkolenia** |  |  |  |
|  | 1. Dostarczenie, uruchomienie/instalacja, konfiguracja i wdrożenie licencji oprogramowania (kont, uprawnień, lokalizacji). 2. Zapewnienie dostępu do aktualizacji i poprawek bezpieczeństwa 3. Świadczenia wsparcia technicznego/serwisowego producenta lub autoryzowanego partnera 4. Przeprowadzenie instruktażu dla administratorów Zamawiającego 5. Tworzenie i wdrażanie polityk bezpieczeństwa (dla stacji, serwerów, mobilnych). 6. Instalacja agentów i modułów ochrony na urządzeniach końcowych. | Tak, podać | Bez oceny |  |
|  | **XVI. Warunki gwarancji i Wsparcie techniczne** |  |  |  |
|  | 1. Objecie oprogramowania gwarancją i wsparciem technicznym Producenta przez okres od dnia 05.03.2026r. do dnia 30.06.2029r. | Tak, podać | Bez oceny |  |
|  | 1. Czas reakcji (tj. diagnostyka i przekazanie informacji o przyczynie wystąpienia błędu krytycznego, błędu zwykłego) – podany w godzinach od momentu zgłoszenia wady, awarii oprogramowania | Tak, podać  (min 1 godz. max. 24 godz.) | Oceniany |  |
|  | 1. Czas naprawy jeśli wada uniemożliwia użytkowanie przedmiotu umowy **(błąd krytyczny)** – podany w dniach od dnia zgłoszenia wad lub awarii przez Zamawiającego | Tak, podać  (min 1 dzień max. 3 dni) | Oceniany |  |
|  | 1. Czas naprawy jeśli wada umożliwia użytkowanie przedmiotu umowy **(błąd zwykły)** - w terminie 14 dni od dnia zgłoszenia wady lub awarii przez Zamawiającego | Tak, podać | Bez oceny |  |
|  | 1. Pozostałe warunki gwarancji i wsparcia technicznego zgodnie z projektem umowy stanowiącym Załącznik nr 11 do SIWZ | Tak, podać | Bez oceny |  |

**Treść oświadczenia Wykonawcy:**

1. Oświadczamy, że przedstawione powyżej dane są prawdziwe oraz zobowiązujemy się do realizacji usługi zgodnie z wyspecyfikowanymi parametrami.
2. Oświadczamy, że oferowany, powyżej wyspecyfikowane oprogramowanie jest kompletne i po zainstalowaniu będzie gotowe do eksploatacji, bez żadnych dodatkowych zakupów i inwestycji.
3. Oświadczamy, że w przypadku wezwania Zamawiającego do przedstawienia/udowodnienia spełnienia kryteriów (praktycznego sprawdzenia funkcjonalności) określonych w niniejszym Załączniku, przedstawimy/zaprezentujemy wymagane funkcjonalności w terminie wskazanym przez Zamawiającego. Przyjmujemy do wiadomości, że brak udowodnienia posiadanej funkcjonalności upoważnia Zamawiającego do odrzucenia oferty.

...........................................................................................

Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy

należy opatrzyć kwalifikowanym podpisem elektronicznym