Signature Not Verified

Dokument podpisany przez
Tomasz Szczepański, CWŻ
Data: 2026.08.10 10:27:22 CEST

CENTRALNY WODOCIĄG ŻUŁAWSKI SP. Z O.O.
ul. Warszawska 28A, 82-100 Nowy Dwór Gdański

Znak sprawy: 3/ZP/2026

Nowy Dwór Gdański, dnia 10.08.2026 r.

WYJAŚNIENIE TREŚCI SWZ ORAZ ZMIANA TREŚCI SWZ/OPZ
- DOPUSZCZENIE ROZWIĄZAŃ RÓWNOWAŻNYCH XDR I NDR -

dot.: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji (art. 275 pkt 1 ustawy Pzp) pn. „Dostawa i wdrożenie sprzętu informatycznego w ramach projektu pn. «Cyberbezpieczne Wodociągi»", znak sprawy 3/ZP/2026.

Zamawiający, działając na podstawie art. 284 ust. 1 i 6 oraz art. 286 ust. 1 i 7 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2026 r. poz. 793, dalej: „ustawa Pzp"), w związku z wnioskiem z dnia 07.08.2026 r. o zmianę SWZ/OPZ poprzez dopuszczenie rozwiązań równoważnych klasy XDR i NDR, udziela poniższego wyjaśnienia i dokonuje zmiany treści dokumentów zamówienia.

TREŚĆ WNIOSKU (bez ujawniania źródła):

Wykonawca wniósł o dopuszczenie, jako rozwiązań równoważnych względem wymagań OPZ, rozwiązań klasy XDR oraz NDR opisanych w tabelach porównawczych załączonych do wniosku, wskazując, że przedstawione rozwiązania realizują zasadnicze cele i wymagane funkcjonalności systemu, a różnice dotyczą przede wszystkim architektury, nazewnictwa funkcji i technicznego sposobu ich realizacji.

STANOWISKO ZAMAWIAJĄCEGO:

Zamawiający uwzględnia wniosek o dopuszczenie rozwiązań równoważnych w zakresie XDR i NDR.

1. Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych klasy XDR oraz NDR, spełniających wymagania określone w Załączniku nr 1 do niniejszego pisma - „Dopuszczona specyfikacja równoważna XDR i NDR".

2. W zakresie pozycji objętych Załącznikiem nr 1 wymagania w nim określone stanowią dopuszczalny, alternatywny sposób spełnienia wymagań OPZ. Wykonawca może zatem zaoferować rozwiązanie zgodne z wymaganiami pierwotnego OPZ albo rozwiązanie równoważne zgodne z wymaganiami określonymi w Załączniku nr 1.

3. Dopuszczenie rozwiązania równoważnego nie oznacza obowiązku łącznego spełnienia przez oferowane rozwiązanie wymagań pierwotnego OPZ oraz alternatywnych wymagań równoważnych w tych samych pozycjach. Ocena zgodności będzie dokonywana odpowiednio według wybranego przez Wykonawcę wariantu rozwiązania.

4. Niniejsza zmiana ma zastosowanie w jednakowym zakresie do wszystkich Wykonawców ubiegających się o udzielenie zamówienia i nie jest ograniczona do podmiotu, który wystąpił z wnioskiem.

5. Pozostałe postanowienia SWZ i OPZ, które nie zostały objęte niniejszą zmianą, pozostają bez zmian i zachowują moc obowiązującą.

6. Niniejsze wyjaśnienie wraz z Załącznikiem nr 1 stanowi integralną część SWZ. W przypadku rozbieżności pomiędzy dotychczasową treścią OPZ a niniejszą zmianą, w zakresie objętym dopuszczeniem rozwiązań równoważnych wiążąca jest treść niniejszego pisma i Załącznika nr 1.

Załącznik nr 1: Dopuszczona specyfikacja równoważna XDR i NDR.

ZAMAWIAJĄCY

XDR Specyfikacja równoważna	XDR specyfikacja obecna
1. Centralna konsola zarządzania w chmurze	
Centralne zarządzanie 1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).	1.4 System musi być zarządzalny zdalnie za pomocą centralnej konsoli chmurowej.
2. Integracja z Active Directory	
Centralne zarządzanie 6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.	1.6 Active Directory: Rozwiązanie musi zapewniać integrację z Active Directory oraz LDAP (usługą katalogową, hierarchiczna baza danych). System musi mieć możliwość wyłącznie jednokierunkowej synchronizacji (wychodzącej) Użytkowników/Grup z lokalnych serwerów Active Directory do Chmurowego (centralnego) Pulpitu Nawigacyjnego w celu zarządzania politykami.
3. Zabezpieczenie konsoli i transmisji protokołem SSL/TLS	
Centralne zarządzanie 4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.	1.10 Bezpieczeństwo danych: Wdrożenie silnych mechanizmów szyfrowania i autentykacji, zapewniających ochronę danych przed nieautoryzowanym dostępem. W tym wsparcie TLS 1.3.
4. Uwierzytelnianie wieloskładnikowe administratorów	

Centralne zarządzanie 10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania. 11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: ➢ Google Authenticator, ➢ Microsoft Authenticator, ➢ Authy, ➢ Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.	1.30 Uwierzytelnienie wieloskładnikowe: Rozwiązanie musi posiadać możliwość zastosowania MFA dla administratorów logujących się do systemu/konsoli chmurowej. Wsparcie Authy, MS Authenticator, Google Authenticator, wiadomości mailowej i SMS.
5. Zarządzanie grupami, politykami i harmonogramami	
Centralne zarządzanie 13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 14. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: ➢ Adresy sieciowe IP.	1.39 Możliwość tworzenia polityk dla użytkowników i urządzeń. Funkcja automatycznego wyłączenia polityki według harmonogramu.

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**

➢ Aktywne zagrożenia. ➢ Stan funkcjonowania oraz ochrony. ➢ Wersja systemu operacyjnego. ➢ Podzespoły komputera. 15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem: ➢ Wyrażenie CRON. ➢ Codziennie. ➢ Cotygodniowo. ➢ Co miesiąc. ➢ Co rok. ➢ Po wystąpieniu nowego zdarzenia. ➢ Po automatycznym umieszczeniu hosta w grupie dynamicznej.	
6. Raportowanie i wizualizacja zagrożeń	
Centralne zarządzanie 12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora. Ochrona stacji roboczych - Windows 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	1.16 Dashboarding: Musi posiadać wysoce modyfikowalny dashboard (widok) z biblioteką widżetów pozwalających na intuicyjną analizę zagrożeń. Rozwiązanie musi pozwalać na skonfigurowanie i możliwość zapisu kilku wcześniej stworzonych dashboardów. 1.38 System musi posiadać funkcję analizy zagrożeń na wykresie.

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.	
7. Eksport danych oraz historii analizy	
Centralne zarządzanie 17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog. 18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach: ➢ JSON. ➢ LEEF. ➢ CEF.	1.44 Rozwiązanie musi być w stanie zapisać historię i analizę przeprowadzonego ataku oraz wyeksportowanie go formatów takich jak SQLite, czy JSON.
8. Wykrywanie zagrożeń i skanowanie w czasie rzeczywistym	

Ochrona stacji roboczych - Windows 3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: ➢ Wirus. ➢ Trojan. ➢ Robak. ➢ Adware. ➢ Spyware. ➢ Dialer. ➢ Phishing. ➢ Backdoor. 9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Ochrona stacji roboczych – MacOS 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: ➢ Wirus. ➢ Trojan. ➢ Robak. ➢ Adware. ➢ Spyware. ➢ Dialer. ➢ Phishing. ➢ Backdoor. 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. Ochrona stacji roboczych – Linux 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: ➢ Wirus.	1.2 Wykrywanie zagrożeń: Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Używać zaawansowanych technik uczenia maszynowego i algorytmów sztucznej inteligencji do wykrywania nowych i rozwijających się zagrożeń. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanego wcześniej złośliwego oprogramowania, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. Wybitnie wysoka skuteczność powinna być potwierdzona w testach organizacji takich jak: Gartner, SE Labs, MITRE itd.

XDR Specyfikacja równoważna	XDR specyfikacja obecna
➢ Trojan. ➢ Robak. ➢ Adware. ➢ Spyware. ➢ Dialer. ➢ Phishing. ➢ Backdoor. 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. Ochrona serwera – Windows Server 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. Ochrona serwera – 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.	
9. Heurystyka, sztuczna inteligencja i głębokie uczenie	

Ochrona stacji roboczych - Windows 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. Ochrona stacji roboczych – MacOS 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. Ochrona stacji roboczych – Linux 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. Ochrona serwera – Windows Server 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,	1.36 Zaawansowany mechanizm głębokiego uczenia (Advanced Deep Learning) a) System musi skanować z ogromną prędkością – w ciągu 20 milisekund model musi być w stanie wyodrębnić miliony cech z pliku, przeprowadzić dogłębną analizę i określić, czy plik jest bezpieczny czy złośliwy. Cały ten proces odbywa się przed wykonaniem pliku. b) Powinien móc przetwarzać dane przez wiele warstw analizy, gdzie każda warstwa znacząco zwiększa moc modelu. c) Model głębokiego uczenia musi być testowany i oceniany kompleksowo przy użyciu zaawansowanych, opracowanych pakietów takich jak Keras, Tensorflow i Scikit-learn.

z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. Ochrona serwera – Linux 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.	
10. Klasyfikacja i blokowanie potencjalnie niepożądanych aplikacji oraz treści	
Ochrona stacji roboczych - Windows 4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	1.7 Klasyfikacja plików i aplikacji: jako złośliwe, potencjalnie niechciane aplikacje (PUA), lub niegroźne oraz posiadać możliwość ich zablokowania. 1.41 Funkcja blokująca pobieranie szkodliwych i niepożądanych treści.
11. Filtrowanie adresów URL	

Ochrona stacji roboczych - Windows 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.	1.8 URL filtering: Usługa pozwalająca na kontrolę dostępu do wybranych stron internetowych oraz stron o danej kategorii i tematyce.

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**
12. Inspekcja ruchu szyfrowanego SSL/TLS	
Ochrona stacji roboczych - Windows 15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.	1.40 Funkcja pozwalająca na inspekcję danych przesyłanych przez SSL/TLS.
13. Blokowanie zewnętrznych nośników i urządzeń	

Ochrona stacji roboczych - Windows 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.	1.15 Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pendrive, urządzeń Bluetooth, modemów.
14. Izolacja sieciowa stacji lub hosta	

Endpoint Detection and Response / eXtended Detection and Response 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.	1.17 Kwarantanna stacji roboczej: Umożliwia automatyczne bądź manualne odizolowanie zainfekowanego urządzenia od sieci, blokując wszystkie połączenia przychodzące i wychodzące. Po zainicjowaniu, jedynie administrator ma dostęp do stacji z poziomu konsoli rozwiązania.
15. Ochrona przed ransomware i przywracanie plików	
Ochrona stacji roboczych - Windows 7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware. ➢ Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych. ➢ Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może	1.25 Ochrona przed Ransomware a) Musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania. b) Zarówno Ochrona Anti-Exploit, jak i Ochrona przed Ransomware nie potrzebują odwołania do Chmury (Cloud Lookup) do wykonania wykrycia. c) Gdy funkcja Anti-crypto podejrzewa, że określone zachowanie nie jest zgodne z zamierzonym procesem, Rejestrator Danych (Data Recorder) zaczyna buforować dane, podczas gdy wspomniane zachowanie jest dokładnie analizowane w celu zidentyfikowania, czy aplikacja jest

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.	bezpieczna, czy aktywność jest uzasadniona. Maksymalny rozmiar rejestratora danych to 200 MB, a minimalny rozmiar pojedynczego pliku, który zostałby zarejestrowany, to 25 MB. d) Funkcja anti-crypto sprawdza wszystkie złośliwe pliki, które zostały zmienione przez złośliwy proces i przywraca je do ich pierwotnej wersji e) Gdyby infekcja ransomware mimo wszystko się przedostała, szczegółowe, historyczne śledzenie tego, skąd infekcja pochodziła i jak się rozprzestrzeniała, zostanie zgłoszone dzięki "Threat Cases" (RCA - analiza przyczyn źródłowych).
16. Ochrona przed rootkitami, bootkitami i zagrożeniami przed startem systemu	
Ochrona stacji roboczych - Windows 5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się. 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego. Ochrona serwera – Windows Server 16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	1.27 Ochrona przed złośliwym oprogramowaniem typu Rootkit (infekującego jądro i usuwającego ukrywane programy z listy procesów oraz plików zwracanych do programów) i Bootkit (złośliwe oprogramowanie uruchomiane w trakcie startu systemu, zaprojektowanego w celu uzyskania niskopoziomowej kontroli nad komputerem bez wiedzy właściciela).
17. Wykrywanie złośliwego ruchu i botnetów	

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**

Ochrona stacji roboczych - Windows 6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.	1.28 Wykrywanie złośliwego ruchu (MTD). System musi być w stanie wykrywać komunikację między komputerami końcowymi a serwerami dowodzenia i kontroli zaangażowanymi w ataki botnetowe lub inne ataki z użyciem złośliwego oprogramowania
18. IDS/IPS i ochrona przed włamaniami	
Ochrona stacji roboczych - Windows 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, ➢ My SQL, ➢ MS SQL. C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	1.13 IPS (Intrusion Prevention System – system wykrywania i zapobiegania włamaniom): System musi być zdolny do monitorowania ruchu poprzez inspekcję pakietów na poziomie endpointa (komputera/stacji roboczej z zainstalowanym oprogramowaniem antywirusowym).
19. HIPS, wykrywanie exploitów i aktywne blokowanie ataków	

Ochrona stacji roboczych - Windows 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. Ochrona serwera – Windows Server 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	1.32 Funkcja pozwalająca na wykrycie ataku hakerskiego prowadzonego w czasie rzeczywistym, poprzez rozpoznanie powszechnie stosowanych narzędzi hakerskich (toolkitów) i potencjalnie szkodliwych zachowań oraz umiejętność aktywnego blokowania ataku w przypadku jego wykrycia. 1.33 Zapobieganie/Wykrywanie dla następujących znanych exploitów: a) Data Execution Protection (DEP) – zapobiega nadużyciu przepełnienia bufora. b) Randomizacja układu przestrzeni adresowej (ASLR) – zapobiega przewidywalnej lokalizacji kodu. c) ASLR "od dołu" (Bottom-up) – ulepszona randomizacja lokalizacji kodu. d) Strona Null (Ochrona przed Dereferencją Null) – powstrzymuje exploity skaczące przez stronę 0. e) Alokacja "Heap Spray" – wstępnie alokuje wspólne obszary pamięci, aby blokować przykładowe ataki. f) Dynamiczne "Heap Spray" – powstrzymuje ataki, które "rozpylają" podejrzane sekwencje na „stercie” (heap). g) "Stack Pivot" – powstrzymuje nadużycie wskaźnika stosu. h) Wykonywanie stosu (MemProt) – powstrzymuje kod atakującego na stosie. i) Środki zaradcze przeciwko ROP opartemu na stosie (Caller) – powstrzymuje standardowe ataki zorientowane na powrót (ROP). j) Środki zaradcze przeciwko ROP opartemu na gałęziach (wspomagane sprzętowo) – powstrzymuje zaawansowane ataki zorientowane na powrót (ROP). k) Ochrona przed nadpisaniem struktury obsługi wyjątków (SEHOP) – powstrzymuje nadużycie procedury obsługi wyjątków. l) Filtrowanie dostępu do tabeli adresów importu (IAF) (wspomagane sprzętowo) – powstrzymuje atakujących, którzy wyszukują adresy API w IAT. m) Wywołania API LoadLibrary – uniemożliwia ładowanie bibliotek ze ścieżek UNC. n) Odbicie iniekcji DLL – uniemożliwia ładowanie

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.	biblioteki z pamięci do procesu hosta. o) Monitorowanie power shell code – wykrywanie wrogiego wdrożenia kodu power shell obejmuje wiele technik adresujących rzeczy takie jak fragmentowany kod power shell, zaszyfrowane ładunki i kodowanie wolne od wartości null. p) VBScript God Mode – musi mieć zdolność wykrywania manipulacji flagą safemode w VBScript w przeglądarce internetowej. q) WoW64 – musi mieć zdolność zabraniania kodowi programu bezpośredniego przełączania z trybu 32-bitowego na 64-bitowy (np. przy użyciu ROP), jednocześnie umożliwiając warstwie WoW64 wykonanie tego przejścia. r) Wywołanie systemowe (Syscall) – powstrzymuje atakujących, którzy próbują ominąć zabezpieczenia. s) Hollow Process Protection – powstrzymuje ataki, które wykorzystują legalne procesy do ukrycia wrogiego kodu. t) Przejęcie DLL (DLL Hijacking) – nadaje priorytet bibliotekom systemowym dla aplikacji pobranych. u) Blokada Aplikacji (Application Lockdown) – automatycznie wyłączy chronioną aplikację na podstawie jej zachowania; na przykład, gdy aplikacja pakietu Office jest wykorzystywana do uruchomienia programu PowerShell, uzyskania dostępu do WMI, uruchomienia makra w celu zainstalowania dowolnego kodu lub manipulowania krytycznymi obszarami systemowymi, rozwiązanie musi zablokować złośliwą akcję – nawet gdy atak nie tworzy procesu potomnego. v) Blokada Java (Java Lockdown) – zapobiega atakom, które nadużywają Javy do uruchamiania plików wykonywalnych Windows. w) Obejście AppLockera "Squiblydoo" – uniemożliwia regsvr32 uruchamianie zdalnych skryptów i kodu.
20. Analiza incydentów oraz telemetria EDR/XDR	

Endpoint Detection and Response / eXtended Detection and Response 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. 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.	1.1 System musi umożliwiać administratorom identyfikację danych dotyczących incydentów bezpieczeństwa, oferując analizę obejmującą charakterystykę ataku, metodę jego inicjacji, konsekwencje oraz strategie odpowiedzi. 1.26 Threat Cases (wcześniej RCA - Root Cause Analysis a) Musi mieć możliwość zidentyfikowania, co się stało, gdzie naruszenie miało początek, jakie pliki zostały naruszone i dostarczyć wskazówek, jak wzmocnić stan bezpieczeństwa organizacji. b) Po wystąpieniu infekcji Threat Cases (RCA) śledzi dane, umożliwiając określenie pochodzenia infekcji, wszelkich wynikających z niej szkód w aktywach, potencjalnie ujawnionych danych oraz łańcucha zdarzeń prowadzących do zatrzymania infekcji. c) Threat Case musi dostarczać podsumowanie zdarzenia: Jaki exploit został odkryty. Gdzie wystąpiło zdarzenie "beacon" (na jakim aktywie). Kiedy wystąpiło. Jak infekcja się powiodła. d) Threat Cases musi dostarczać rekomendacje do rozwiązania problemu: Rzeczy, których należy szukać po ataku. Np. Poza tym, że pliki zostały przywrócone po zaszyfrowaniu, sprawdź ustawienia przeglądarki, aby upewnić się, że nie powstały żadne luki w zabezpieczeniach w wyniku infekcji. e) "Activity Record" pozwala administratorom dodawać notatki do sprawy. Wszystkie notatki związane ze sprawą będą wymienione w tej kolumnie. f) Istnieją również przyciski umożliwiające administratorowi zmianę statusu sprawy (Nowa, W toku, Zamknięta) i ustawienie priorytetu (Niski, Średni, Wysoki). Podczas zamykania administrator może dodać notatki i potwierdzić (za pomocą pól wyboru), że podjęto kroki zaradcze: przeanalizowano wpływ na pliki/aktywa i wdrożono odpowiednie ulepszenia środowiskowe. g) Zapewnia widok tabelaryczny wszystkiego, co zostało naruszone podczas ataku. Elementy można filtrować na podstawie typu, np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdym elemencie, np. nazwa pliku (pliki ofiary lub agent złośliwego oprogramowania), ID procesu,

	znacznik czasu rozpoczęcia/zatrzymania zdarzenia. h) Threat Cases musi wyraźnie wskazywać początek przyczyny źródłowej, przedstawiając serię zdarzeń wynikających z ataku jako zbiór węzłów. Każdy węzeł zawiera szczegółowe informacje o plikach, procesach, kluczach rejestru itp. zaangażowanych na tym etapie. Zdarzenie "beacon" zostanie zidentyfikowane w łańcuchu, ale pokazane zostaną również wszelkie zdarzenia wykonane przez proces zidentyfikowany jako zdarzenie "beacon". i) Threat case musi mieć możliwość żądania najnowszych informacji

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**
21. Listy wykluczeń oraz białe i czarne listy	

Ochrona stacji roboczych - Windows 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). Endpoint Detection and Response / eXtended Detection and Response 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.	1.29 White & Black Listing dla wersji serwerowej agenta: Możliwość skonfigurowania białej i czarnej listy usług w celu zawężenia liczby dostępnych usług.
22. Monitorowanie skryptów i PowerShell	

Endpoint Detection and Response / eXtended Detection and Response 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.	1.12 AMSI: Ochrona przed szkodliwym kodem (np. skrypty PowerShell).
23. Szyfrowanie dysków	

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	1.37 Funkcja pozwalająca na zaszyfrowanie oraz odszyfrowanie dysku urządzenia oraz wymianę haseł przez konsolę administratora/chmurową.

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.	
24. Zapora sieciowa	

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**

Ochrona stacji roboczych - Windows 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.	1.42 Musi poprawnie współpracować z Windows Firewall.
25. Obsługiwane systemy operacyjne	

Ochrona stacji roboczych - Windows 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). Ochrona stacji roboczych – MacOS 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych. Ochrona stacji roboczych – Linux 1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: ➢ Ubuntu Desktop, ➢ Red Hat Enterprise Linux ➢ Linux Mint. Ochrona serwera – Windows Server 1. Rozwiązanie musi wspierać systemy w tym co najmniej: ➢ Microsoft Windows Server 2012 R2, ➢ Microsoft Windows Server 2016, ➢ Microsoft Windows Server 2019, ➢ Microsoft Windows Server 2022, ➢ Microsoft Windows Server 2025. 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. Wymagania systemowe: a) Rozwiązanie jest dostępne na wielu wersjach systemów operacyjnych (w tym aktualnej): i. Windows 11 & 10 (64-bit) ii. Windows Server 2012 i nowsze iii. Mac OS 13 i nowsze iv. Linux: • Amazon Linux 2 • Amazon Linux 2023 • CentOS 7 (3.10.0-1062 lub późniejsze) • CentOS Minimal • CentOS Stream • Debian 10 • Debian 11 • Debian 12 • Debian 13 • Miracle Linux 8 • Oracle 7 (UEK 4.14 lub późniejsze, RHCK 3.10.0-1062 lub późniejsze) • Oracle 8 • Oracle 9 • Oracle 10 • RHEL 7 (3.10.0-1062 lub późniejsze) • RHEL 8 • RHEL 9 • RHEL 10 • SUSE Linux Enterprise Server 12 • SUSE Linux Enterprise Server 15 • Ubuntu 18.04 (LTS) (4.15 lub późniejsze) • Ubuntu 20.04 (LTS) • Ubuntu 22.04 (LTS) • Ubuntu 24.04 (LTS) • Ubuntu Minimal
26. Obsługa urządzeń mobilnych Android i iOS	

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.	2. Wymagania systemowe: b) Rozwiązanie powinno także oferować możliwość rozszerzenia licencji o wersje mobilne działające na systemach: i. Android ii. iOS
27. Aktualizacje, harmonogramy i lokalna pamięć podręczna	
Centralne zarządzanie 8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej: ➢ Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania. ➢ Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta. ➢ Buforowanie ruchu HTTPS. 15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem: ➢ Wyrażenie CRON. ➢ Codziennie. ➢ Cotygodniowo. ➢ Co miesiąc. ➢ Co rok. ➢ Po wystąpieniu nowego zdarzenia.	4. Wsparcie i aktualizacje: b) Aktualizacja punktów końcowych powinna umożliwiać ustawienie wstępnie skonfigurowanej dostępnej przepustowości wykorzystywanej zarówno do aktualizacji oprogramowania, jak i aktualizacji definicji zagrożeń (np. 64, 128, 256 Kbps itp.). c) Musi istnieć opcja skonfigurowania lokalnego serwera pamięci podręcznej aktualizacji (cache) w środowisku sieci lokalnej (on-premise) w celu zminimalizowania pobierania dużych aktualizacji oprogramowania. d) Należy mieć możliwość dodania Zasad Zarządzania Aktualizacjami, aby umożliwić ustawienie harmonogramów aktualizacji na punkcie końcowym.

➢ Po automatycznym umieszczeniu hosta w grupie dynamicznej.	

XDR Specyfikacja równoważna	**XDR specyfikacja obecna**
Ochrona serwera – Windows Server 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. Ochrona serwera – Linux 5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.	
28. Wsparcie techniczne	
Wsparcie techniczne. 1. Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.	4. Wsparcie i aktualizacje: a) Wsparcie techniczne producenta na czas trwania licencji.
29. Jednoproducentowość rozwiązania	

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. Szyfrowanie 1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. Mobile Device Management 2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.	1.20 Unifikacja: Rozwiązanie musi w całości pochodzić od jednego producenta. Użycie połączenia kilku produktów w celu spełnienia warunków specyfikacji technicznej jest zabronione.
30. Integracja z Google Workspace i Microsoft 365	
Ochrona usług chmurowych 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.	5. Integracje: 5.6 Możliwość integracji dla celów automatyzacji odpowiedzi na incydenty cyberbezpieczeństwa z wiodącymi rozwiązaniami takimi jak: • Google Workspace • Microsoft 365 Management Activity • Microsoft 365 Response Actions • MS Graph Security API (Legacy) • MS Graph Security API V2
31. Integracja z AWS	
Ochrona serwerów w chmurze AWS, Microsoft Azure i Google Cloud Platform 2. Rozwiązanie musi udostępniać możliwość integracji przynajmniej z rozwiązaniami: ➢ Microsoft Azure. ➢ Google Cloud Platform.	5. Integracje: 5.7 Możliwość integracji z następującym wiodącymi rozwiązaniami dostawców cyberbezpieczeństwa i chmury publicznej: • AWS

➢ Amazon Web Services.	

NDR

NDR Specyfikacja równoważna	**NDR Specyfikacja Obecna**
1. Monitorowanie ruchu sieciowego i wykrywanie zagrożeń	
NDR Opis techniczny Rozwiązanie do monitorowania i wykrywania zagrożeń pojawiających się w sieci komputerowej, na podstawie analizy pełnej kopii ruchu sieciowego (NDR).	1. System musi monitorować aktywność sieci w czasie rzeczywistym i identyfikować potencjalne cyberzagrożenia, ryzyka cyberbezpieczeństwa i anomalie oraz generować o nich alerty w czasie rzeczywistym.
2. Praca lokalna (on-prem / offline)	
1. Rozwiązanie musi w pełni realizować swoje funkcje lokalnie (on-prem).	5. System powinien być w pełni funkcjonalny w środowisku offline klienta bez użycia środowiska chmury do gromadzenia, przechowywania i przetwarzania danych, a wszystkie konfiguracje i raporty powinny być dostępne bezpośrednio w systemie.
3. Wdrożenie w środowisku wirtualnym i skalowalność	

2. Rozwiązanie musi być zainstalowane i uruchomione na dedykowanych urządzeniach dostarczonych wraz z platformą, lub umożliwiać instalację na platformie wirtualizacji, z wykorzystaniem platformy Vmware lub Proxmox. 7. Sondę można zaimplementować w kompatybilnym środowisku wirtualnym. 12. W przypadku dostawy z wykorzystaniem wirtualizacji system a. umożliwia dowolne skalowanie, w postaci możliwości implementacji dodatkowych sond monitorujących, bez ponoszenia dodatkowych kosztów.	Należy dostarczyć i wdrożyć system do dwóch niezależnych lokalizcji fizycznych. Systemy w obu lokalizacjach muszą pracować w pełni niezależnie. Do obu lokalizacji należy dostarczyć rozwiązanie w formie maszyny wirtualnej (virtual appliance) będące centralnym kolektorem i sensorem. Oczekiwana skalowalność dla lokalizacji A: do 500 monitorowanych hostów oraz do 500 Mb/s analizowanej przepustowości ruchu sieciowego. Oczekiwana skalowalność dla lokalizacji B: do 200 monitorowanych hostów oraz do 100 Mb/s analizowanej przepustowości ruchu sieciowego.

NDR Specyfikacja równoważna	**NDR Specyfikacja Obecna**
b. wydajność zestawu jest zależna od ilości alokowanych zasobów	
4. Pozyskiwanie pełnej kopii ruchu przez SPAN/TAP bez agentów	
8. Sonda odbiera dane w formie pełnej kopii ruchu sieciowego (full package capture), np. dostarczanych poprzez wykorzystanie technologii port mirroringu (span port) na przełącznikach sieciowych lub urządzeniach typu traffic access point (TAP).	2. Dostarczony system musi analizować sieć na podstawie lustrzanego ruchu sieciowego z portów SPAN lub TAP (nie tylko protokołów statystycznych, takich jak NetFlow), bez konieczności wdrażania agentów na punktach końcowych lub innych węzłach sieciowych/hostach.
5. Analiza zawartości pakietów, DPI i parsowanie	

3. Wstępna analiza musi się odbywać zgodnie z mechanizmem parsowania (analizy składniowej danych). ii. wstępna weryfikacja przechwyconego ruchu, pod kątem podatności, realizowana za pomocą mechanizmów traffic payloads opartych o analizę formalną i statystyczną;	3. System musi analizować zawartość pakietów danych w czasie rzeczywistym i wykrywać protokół lub aplikację na podstawie zawartości ruchu poprzez Deep Packet Inspection (DPI), a nie tylko numeru portu.
6. Obsługa IPv4, IPv6 oraz VLAN/802.1Q	
9. Sonda musi wspierać protokoły IPv4, IPv6 i 802.1Q.	• zmiana sieci VLAN, 3. Samouczenie jest wymagane na wszystkich urządzeniach sieciowych i uruchomionych na nich usługach (numery portów od 0 do 65535 zarówno dla TCP, jak i UDP) w protokołach IPv4 i IPv6 oraz innych protokołach warstwy sieciowej L3 i L4.
7. Obsługiwane protokoły aplikacyjne	
4. Oprogramowanie musi mieć możliwość obsługi następujących protokołów: DCERPC, DHCP, DNP3, DNS_udp, DNS_tcp, ENIP, FTP, HTTP, HTTP/2, IKEv2, Kerberos (KRB5), MQTT, NFS, RDP, RFB, SIP, SMB, SMTP, SNMP, SSH, TFTP, TLS.	2. Wymagane protokoły do przechowywania metadanych aplikacji z poszczególnych transakcji to DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, enkapsulacja SSL/TLS.
8. Obsługa protokołów przemysłowych OT	
4. Oprogramowanie musi mieć możliwość obsługi następujących protokołów: DCERPC, DHCP, DNP3, DNS_udp, DNS_tcp, ENIP, FTP, HTTP, HTTP/2, IKEv2, Kerberos (KRB5), MQTT, NFS, RDP, RFB, SIP, SMB, SMTP, SNMP, SSH, TFTP, TLS.	Wspierane protokoły OT 1. Wykrywanie i analizowanie dla protokołów przemysłowych: BACnet, CC-link, COAP, DLMS/COSEM, DNP3, ENIP, EtherCAT, GE-SRTP,

	HART-IP, HL7, IEC-104, IEC61850 (GOOSE,SV, MMS), MODBUS, MQTT, OMRON, FINS, OPC UA, Profinet IO DCE/RPC, PROFINET-DCP, Siemens S7
9. Architektura sond monitorujących i urządzenia administrującego	
3. Architektura musi być oparta o dwa podstawowe elementy składowe: a. Fizyczne lub wirtualne sondy monitorujące, których rolą jest: i. odbieranie kopii ruchu sieciowego na dedykowanych portach monitorujących, wykonanych w standardzie SFP (small form-factor pluggable), umożliwiających podłączenie transceivera (wkładki, modułu) w trybie hot-plugging lub na dedykowanych portach elektrycznych RJ45; ii. wstępna weryfikacja przechwyconego ruchu, pod kątem podatności, realizowana za pomocą mechanizmów traffic payloads opartych o analizę formalną i statystyczną; iii. przekazywanie wstępnie przetworzonego strumienia do urządzenia nadrzędnego (w postaci metadanych); iv. generowanie alarmów oraz/lub metadanych o zdarzeniach; v. odtwarzanie plików w standardzie .pcap; vi. raportowanie informacji o stanie sondy do urządzenia nadrzędnego. b. Fizyczne lub wirtualne urządzenie administrujące, do którego zadań należy: i. zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu;	Do obu lokalizacji należy dostarczyć rozwiązanie w formie maszyny wirtualnej (virtual appliance) będące centralnym kolektorem i sensorem.

ii. dogłębna analiza odebranych plików w oparciu o: - analizę shellcodes; - inżynierię wsteczną;	

NDR Specyfikacja równoważna	NDR Specyfikacja Obecna

- ROP (Return Oriented Programming); - JOP (Jump Oriented Programming); - heurystykę w czasie rzeczywistym; - statyczne silniki malware w ilości minimum 1 sztukI. iii. zarządzanie systemem i podległymi sondami; iv. prezentacja wyników analiz (detekcji) w postaci wykresów i scoringu; v. moduł przechowywania metadanych na potrzeby dalszej analizy (tzw. threat hunting); vi. przekazywanie danych o zagrożeniach do rozwiązań stron trzecich, między innymi rozwiązań typu SIEM. c. oprogramowanie narzędziowe instalowane na sondach monitorujących i urządzeniu administrującym, umożliwiające realizację troubleshootingu z poziomu urządzenia administrującego – aktywność portów, wolumen ruchu dla portów monitorujących, obciążenie elementów systemu, stan kanału do wymiany danych między sondą (sondami), a urządzeniem administrującym. 4. Urządzenie administrujące ma możliwość podpięcia jednocześnie wielu sond monitorujących.	
10. Przetwarzanie i przechowywanie metadanych oraz przepływów	

iii. przekazywanie wstępnie przetworzonego strumienia do urządzenia nadrzędnego (w postaci metadanych); v. moduł przechowywania metadanych na potrzeby dalszej analizy (tzw. threat hunting);	Przetwarzanie i przechowywanie przepływów sieciowych 1. System przechowuje przepływy sieciowe w formacie umożliwiającym analizę komunikacji sieciowej na poziomie poszczególnych przepływów, w tym śledzenie informacji o transakcjach aplikacji i ich metadanych od L2 do L7 zawartych w danym przepływie sieciowym. 2. Wymagane protokoły do przechowywania metadanych aplikacji z poszczególnych transakcji to DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, enkapsulacja SSL/TLS.
11. Pełne przechwytywanie ruchu i obsługa plików PCAP	
8. Sonda odbiera dane w formie pełnej kopii ruchu sieciowego (full package capture), np. dostarczanych poprzez wykorzystanie technologii port mirroringu (span port) na przełącznikach sieciowych lub urządzeniach typu traffic access point (TAP). v. odtwarzanie plików w standardzie .pcap;	Pełne rejestrowanie ruchu, przechowywanie i analiza wsteczna 1. Wymagane jest opcjonalne rejestrowanie pełnego ruchu sieciowego (pełne przechwytywanie pakietów) w formacie PCAP w oparciu o co najmniej następujące parametry: docelowy i źródłowy adres IP/MAC, podsieć, używany protokół, IPv4 lub IPv6. Przechwytywanie może być włączane automatycznie zgodnie z wykrytymi już zdarzeniami lub poprzez aktywację przez użytkownika. 2. Wymagana jest możliwość importowania pliku PCAP za pośrednictwem interfejsu webowego i analizowania go z powrotem za pomocą wszystkich środków wykrywania i analizy kolektora.
12. Wydajność i skalowanie rozwiązania	

12. W przypadku dostawy z wykorzystaniem wirtualizacji system a. umożliwia dowolne skalowanie, w postaci możliwości implementacji dodatkowych sond monitorujących, bez ponoszenia dodatkowych kosztów. b. wydajność zestawu jest zależna od ilości alokowanych zasobów 2. Fizyczne urządzenie administrujące w zależności od modelu: a. obsługuje do 2000 / 4000 / 6000 / 8000 zdarzeń na sekundę b. przechowywanie do 1 / 10 / 80 / 300 milionów zdarzeń c. analizuje przy pomocy silników detekcji malware do 10 /20 / 30 / 50 plików na sekundę d. analizuje przy pomocy silnika detekcji shellcode/powershell do 1 / 2 / 5 / 10 na sekundę e. możliwość konfiguracji architektury typu single-tenant i multi-tenant.	Oczekiwana skalowalność dla lokalizacji A: do 500 monitorowanych hostów oraz do 500 Mb/s analizowanej przepustowości ruchu sieciowego. Oczekiwana skalowalność dla lokalizacji B: do 200 monitorowanych hostów oraz do 100 Mb/s analizowanej przepustowości ruchu sieciowego.
13. Monitorowanie stanu i wydajności systemu oraz sieci	

NDR Specyfikacja równoważna	NDR Specyfikacja Obecna

c. oprogramowanie narzędziowe instalowane na sondach monitorujących i urządzeniu administrującym, umożliwiające realizację troubleshootingu z poziomu urządzenia administrującego – aktywność portów, wolumen ruchu dla portów monitorujących, obciążenie elementów systemu, stan kanału do wymiany danych między sondą (sondami), a urządzeniem administrującym.	Monitorowanie wydajności aplikacji i sieci 1. System mierzy i tworzy automatycznie (bez potrzeby ręcznego ustawiania wartości progowych) model normalnego zachowania dla parametrów wydajności w całej monitorowanej sieci, dla wszystkich urządzeń i we wszystkich usługach, co najmniej: • przepustowość sieci, • szybkość reakcji aplikacji, • reakcja systemu z perspektywy użytkownika. 2. Obliczanie powyższych parametrów wydajności i automatyczne wykrywanie anomalii w oparciu o odchylenia od normalnego modelu zachowania musi być wykonane dla: • wszystkie porty i usługi TCP, • dla wszystkich kombinacji usług i hostów 3. System musi mierzyć informacje o retransmisji pakietów, pakietach poza kolejnością, TTL, QoS i ruchu blokowanym przez firewalle w całej monitorowanej sieci, między wszystkimi urządzeniami i we wszystkich usługach.
14. Konsola webowa i graficzny interfejs użytkownika	

1. Rozwiązanie posiada dostępne poprzez zabezpieczone połączenie (HTTPS) w przeglądarce: a. Konsolę NDR, która: i. Zawiera informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, silnik detekcji odpowiedzialny za wykrycie, sygnatury czasowe ii. Zapewnia podgląd na zdarzenia w formie przeglądów odnosząc się do najważniejszych wydarzeń, assetów, użytkowników (bez konieczności instalacji agenta) iii. Szacuje poziom ryzyka dla każdego wykrytego zagrożenia, w oparciu o dedykowany algorytm iv. Zagrożenia mapowane są w odniesieniu do jednego z tzw. framework'ów (np. MITRE) opisującego znane i wykorzystywane taktyki w kontekście cyberataków v. Daje możliwość tagowania zdarzeń i załączania opisu, notatek b. Konsolę Administracyjną, która: i. Umożliwia kontrolę stanu urządzeń i wykorzystania zasobów ii. Zbieranie danych diagnostycznych iii. Konfigurację eksportu danych	Interfejs użytkownika 1. System powinien zapewniać pojedynczy graficzny interfejs użytkownika dla wszystkich działań użytkownika, w tym wykrywania, analizy statystyk sieciowych, konfiguracji systemu, konfiguracji alertów, raportów i pulpitów nawigacyjnych.

iv. Konfigurację ustawień komponentu uczenia maszynowego v. Konfigurację ustawień komponentu antymalware vi. Konfigurację ustawień komponentu analizy ruchu sieciowego, w tym jego modyfikację, dodawanie źródeł definicji reguł vii. Zarządzanie kontami użytkowników viii. Parowanie urządzenia administrującego z sondami c. Zaimplementowane rozwiązanie umożliwiające katalogowanie zebranych detekcji i dokonywanie ich korelacji na bazie wieloczynnikowych filtrów	
15. Profile, konta użytkowników i uprawnienia	

7. Zarządzanie dostępem a. rozwiązanie musi umożliwiać tworzenie wielu kont użytkowników b. każde konto użytkownika wymaga:	2. System musi umożliwiać tworzenie profili i grup użytkowników w celu ograniczenia funkcjonalności produktu i widoczności przechowywanych danych z obsługą co najmniej: • granularne ustawienia dostępu do analitycznych i konfiguracyjnych/administracyjnych komponentów systemu ze zdefiniowanymi poziomami dostępu (co najmniej odczyt, zapis, wykonanie),

NDR Specyfikacja równoważna	**NDR Specyfikacja Obecna**
i. Nazwy konta ii. Hasła iii. Adresu e-mail iv. Imię v. Nazwisko c. Konta użytkowników muszą mieć zróżnicowane uprawnienia dostępowe do danych oraz modyfikacji ustawień, system musi mieć możliwość zdefiniowania przynajmniej trzech poziomów uprawnień: administratora, użytkownika uprzywilejowanego oraz operatora. d. zarządzanie dostępem musi umożliwiać wykorzystanie protokołu LDAP; e. system musi umożliwiać przechowywanie historii autentykacji.	• granularne ustawienia dostępu do danych z różnych segmentów sieci organizacji ze zdefiniowanymi poziomami dostępu (co najmniej indywidualne i grupy hostów, czujników i podsieci), • tworzenie niestandardowych filtrów dla wszystkich danych i udostępnianie ich użytkownikom i grupom użytkowników, • tworzenie niestandardowych widoków użytkownika, raportów, pulpitów nawigacyjnych itp.

16. Prezentacja zdarzeń, zasobów i informacji kontekstowych	
a. Konsolę NDR, która: i. Zawiera informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, silnik detekcji odpowiedzialny za wykrycie, sygnatury czasowe ii. Zapewnia podgląd na zdarzenia w formie przeglądów odnosząc się do najważniejszych wydarzeń, assetów, użytkowników (bez konieczności instalacji agenta)	Informacje kontekstowe 1. System musi być w stanie pozyskiwać, wizualizować i wyświetlać wymienione informacje kontekstowe dla każdego urządzenia w jednym widoku graficznym: • Nazwa użytkownika i inne parametry z kontrolera domeny (MS Active Directory), w tym jego historia • Nazwa hosta urządzenia i jego historia na podstawie przetwarzania odpowiednich danych z ruchu DNS i DHCP • Geolokalizacja IP • Reputacja adresu IP, w tym informacja, czy adres IP znajduje się na czarnej liście lub jest podejrzany • Historia używanego adresu MAC i producenta urządzenia • System operacyjny i jego historia na urządzeniu • Notatki i informacje o urządzeniu wprowadzone przez użytkownika • Automatycznie przypisane tagi urządzeń, które opisują ich przeznaczenie i zachowanie - co najmniej serwer kontrolera domeny, serwer WWW, serwer poczty, serwer DNS, serwer SSH, serwer bazy danych, drukarka, urządzenie administratora, przechowywanie danych, aktywne śledzenie, skanery podatności i systemy technologiczne. • Lista usług (klienckich i serwerowych) uruchomionych i używanych na urządzeniu oraz ilość przesłanych przez nie

	danych. • Lista wykrytych zdarzeń związanych z bezpieczeństwem i działaniem urządzenia.
17. Tagowanie, opisy i notatki	
v. Daje możliwość tagowania zdarzeń i załączania opisu, notatek	• Notatki i informacje o urządzeniu wprowadzone przez użytkownika • Automatycznie przypisane tagi urządzeń, które opisują ich przeznaczenie i zachowanie - co najmniej serwer kontrolera domeny, serwer WWW, serwer poczty, serwer DNS, serwer SSH, serwer bazy danych, drukarka, urządzenie administratora, przechowywanie danych, aktywne śledzenie, skanery podatności i systemy technologiczne.

18. Katalogowanie, korelacja, wyszukiwanie i threat hunting	
v. moduł przechowywania metadanych na potrzeby dalszej analizy (tzw. threat hunting); c. Zaimplementowane rozwiązanie umożliwiające katalogowanie zebranych detekcji i dokonywanie ich korelacji na bazie wieloczynnikowych filtrów	Wyszukiwanie, filtrowanie i wizualizacja danych 1. System musi być zdolny do natychmiastowego (w ciągu kilku sekund) wyszukiwania i wizualizacji w celu analizy śledczej i wsparcia w poszukiwaniu zagrożeń bez specjalnego języka zapytań. 2. Istnieje możliwość natychmiastowego filtrowania i przeszukiwania pełnej historii wszystkich przechowywanych danych, tj. zdarzeń bezpieczeństwa, przepływów sieciowych i zagregowanych statystyk sieciowych (tabele i wykresy): • według parametrów adres IP i MAC, nazwa hosta, nazwa użytkownika (tożsamość użytkownika), ruch przychodzący i wychodzący, usługa sieciowa, usługa lokalna lub

NDR Specyfikacja równoważna	**NDR Specyfikacja Obecna**
	zdalna (usługa z perspektywy klienta lub serwera), numer portu, VLAN, kraj, ASN, • poprzez wyszukiwanie pełnotekstowe w danych i wyszukiwanie oparte na definicji kierunku (źródło, miejsce docelowe) oraz wyrażeniach logicznych i, lub, nie. 3. System musi zapewniać wstępnie obliczone wartości wydajności i charakterystyki behawioralnej dla każdego urządzenia w sieci i dla wszystkich uruchomionych na nim usług, bez konieczności przetwarzania surowych danych z dzienników sieciowych.

	4. System musi umożliwiać filtrowanie i wizualizację wyników w postaci wykresów, sortowalnych tabel wyliczeniowych i statystyk TOP N.
19. Wizualizacja wyników analiz i przepływów	
iv. prezentacja wyników analiz (detekcji) w postaci wykresów i scoringu;	4. System musi umożliwiać filtrowanie i wizualizację wyników w postaci wykresów, sortowalnych tabel wyliczeniowych i statystyk TOP N. 6. System umożliwia łatwą i natychmiastową wizualizację przepływów sieciowych pomiędzy urządzeniami i podsieciami. Widoki wizualizacji można dowolnie modyfikować za pomocą filtra danych użytkownika.
20. Generowanie alertów i powiadomień	
iv. generowanie alarmów oraz/lub metadanych o zdarzeniach;	Automatyczne raportowanie (alerty) i raportowanie 1. System musi być w stanie powiadomić użytkownika za pośrednictwem co najmniej wiadomości e-mail i dziennika. 2. Alerty muszą być dostarczane przez system w formacie nadającym się do odczytu maszynowego do wykorzystania w narzędziach SIEM i muszą zawierać co najmniej pełne informacje o wykrytym zdarzeniu, w tym łącze URL do zdarzenia w okresie raportowania w interfejsie graficznym systemu.
21. Raportowanie	

9. Raportowanie: a. pozwala na utworzenie raportu zawierającego podsumowanie zagrożeń, alertów, użytkowników i domen, b. raport musi zawierać informacje z okresu 24h, 7 dni i 31 dni, c. raport musi pozwalać na zapis w formacie docx.	Automatyczne raportowanie (alerty) i raportowanie 1. System musi być w stanie powiadomić użytkownika za pośrednictwem co najmniej wiadomości e-mail i dziennika. 2. Alerty muszą być dostarczane przez system w formacie nadającym się do odczytu maszynowego do wykorzystania w narzędziach SIEM i muszą zawierać co najmniej pełne informacje o wykrytym zdarzeniu, w tym łącze URL do zdarzenia w okresie raportowania w interfejsie graficznym systemu. 3. Wymagane jest tworzenie automatycznych raportów
22. Integracja z SIEM i rozwiązaniami zewnętrznymi (API / syslog)	
vi. przekazywanie danych o zagrożeniach do rozwiązań stron trzecich, między innymi rozwiązań typu SIEM. 8. Udostępnianie danych do rozwiązań stron trzecich: a. rozwiązanie musi umożliwiać definiowanie automatycznej synchronizacji zebranych danych i detekcji do innych rozwiązań poprzez API; b. rozwiązanie musi umożliwiać rejestrowanie i przesyłanie informacji o zdarzeniach zachodzących w systemie (logów systemowych) w standardzie syslog do zewnętrznego serwera.	Integracja systemu 1. System musi zapewniać co najmniej gotowe narzędzia, które umożliwiają integrację z oprogramowaniem innych firm bez korzystania z interfejsu API systemu: • syslog, CEF i LEEF do eksportu zdarzeń, w tym pełna obsługa filtrów (eksport tylko wymaganych danych) • bezpośrednie linki URL do dowolnego ekranu GUI i filtrowanych widoków w GUI • eksportowanie informacji o przepływie w formacie IPFIX lub podobnym, w tym pełna obsługa filtrów (można eksportować tylko wymagane dane), w tym metadane aplikacji dla co najmniej protokołów HTTP, HTTPS i SMTP • integracja z usługami tożsamości użytkowników bez

	konieczności konfigurowania wysyłania logów do systemu - przynajmniej Cisco ISE i Microsoft Active Directory • Integracja z zaporami sieciowymi, co najmniej Cisco, Palo Alto, Fortinet i Checkpoint, w celu automatycznego i ręcznego reagowania wyzwalanego przez system. • Integracja z narzędziami kontroli dostępu do sieci, co najmniej Cisco ISE, w celu automatycznej i ręcznej reakcji systemu.
23. Wykrywanie złośliwego oprogramowania z użyciem analiz statycznych i heurystycznych	
4. Rozwiązanie obsługuje następujące silniki detekcji: a. antymalware – skan plików w ruchu sieciowym w celu identyfikacji szkodliwego oprogramowania, realizowany poprzez co najmniej 15 niezależnych silników detekcji, przy użyciu analiz statycznych i heurystycznych; b. silniki skanowania w poszukiwaniu zagrożeń typu malware powinny obsługiwać również mechanizm skanowania plików sklasyfikowanych jako podejrzane, z użyciem	Wykrywanie na podstawie bazy danych znanych zagrożeń 1. System musi być w stanie identyfikować zagrożenia i zgłaszać zdarzenia na podstawie: • baza danych wykrywania znanych zagrożeń, tj. złośliwego oprogramowania (trojanów, wirusów, robaków, rootkitów itp.), znanych ataków (exploitów) i luk w zabezpieczeniach, naruszeń zasad bezpieczeństwa i "najlepszych praktyk" oraz innych zagrożeń,

NDR Specyfikacja równoważna	**NDR Specyfikacja Obecna**

nowych sygnatur po aktualizacji silnika detekcji;	• baza danych znanych złośliwych adresów IP, rekordów DNS i nazw hostów, adresów URL i skrótów plików.
24. Przekazywanie podejrzanych plików do dalszej analizy / Sandbox	
2. Rozwiązanie musi mieć możliwość przesłania podejrzanych plików w celu przeskanowania pod kątem zawierania szkodliwego oprogramowania, powershell i shellcode.	Wykrywanie przy użyciu Sandbox 1. System musi umożliwiać integrację z systemem Sandbox w celu analizy statycznej i dynamicznej, tzw. detonacji w środowisku wirtualnym. 2. W przypadku integracji, system musi być w stanie przekazywać pliki i adresy url do Sandbox w celu dalszej analizy. 3. System musi być w stanie wyświetlić wynik analizy Sandbox we własnym środowisku graficznym, wraz z innymi zdarzeniami.
25. Reguły i sygnatury detekcji	
3. Rozwiązanie musi mieć możliwość definiowania reguł zarówno w sondach, jak i centralnie, w urządzeniu administrującym. d. analiza ruchu w oparciu o definicje zagrożeń – analiza całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń, musi umożliwiać dodawanie i modyfikowani dodawanie własnych sygnatur ataków;	5. Baza reguł wykrywania (sygnatur) musi być oparta na zaawansowanych wyrażeniach regularnych do przetwarzania ciągów znaków, które mogą sprawdzać całą komunikację sieciową od L2 (Ethernet itp.) do L7. System musi wykrywać zdarzenia w oparciu o dużą liczbę reguł sygnatur (co najmniej kilkadziesiąt tysięcy). 6. Użytkownik musi mieć możliwość dodawania własnych reguł wykrywania za pośrednictwem aplikacji internetowej w praktycznym i powszechnie używanym formacie bez konieczności znajomości składni i semantyki reguł. Przykład możliwej składni reguły wykrywania: alert tcp $HOME_NET any -> any any (msg: "Command Shell Access";

	content: "C:\\Users\\\Administrator\\\Desktop\\\hfs2.3b";)
26. Wykrywanie DGA, komunikacji C&C i botnetów	
e. domain generation algorithm (DGA) – wykrywanie losowego generowanie domen, które są używane do okresowego generowania dużej liczby nazw domen, które mogą być używane jako odnośniki do połączeniami z serwerami C&C (Command and Control).	1. System musi być w stanie wykrywać nieznane zagrożenia, których nie można zidentyfikować za pomocą sygnatur wykrywania, takie jak trojany, botnety itp. W szczególności należy zidentyfikować następujące oznaki potencjalnie złośliwego zachowania: • działania związane z eksploracją sieci, • wykrywanie podejrzanych zachowań maszyn, które nie są generowane przez ludzkich użytkowników sieci, • wykrywanie powtarzających się wzorców zachowań w sieci, • wykrywanie botnetów i kontrola zagrożonych stacji, • ataki typu brute-force i wyliczanie danych, • baza danych znanych złośliwych adresów IP, rekordów DNS i nazw hostów, adresów URL i skrótów plików.
27. Definiowanie zakresów sieci i zasad bezpieczeństwa	

1. Możliwość definiowania zasad detekcji i wykrywania zagrożeń. 2. Możliwość definiowania zakresów sieci: a. na podstawie adresacji IP; b. na podstawie VLAN.	2. Do celów monitorowania polityki cyberbezpieczeństwa system musi zapewniać użytkownikowi narzędzie do definiowania reguł przy użyciu: • podsieci zdefiniowane przez użytkownika na podstawie zakresów adresów IP • Grupy urządzeń zdefiniowane przez użytkownika • automatycznie przypisane tagi urządzeń, które opisują ich przeznaczenie i zachowanie - co najmniej serwer kontrolera domeny, serwer WWW, serwer poczty, serwer DNS, serwer SSH, serwer bazy danych, drukarka, urządzenie administratora, przechowywanie danych, aktywne śledzenie, skanery podatności i systemy technologiczne.
28. Szyfrowana komunikacja i analiza TLS	
6. Połączenie pomiędzy urządzeniem administrującym a sondą realizowane jest poprzez bezpieczne (szyfrowane) połączenie na bazie protokołu IPSec.	7. Analiza szyfrowanej komunikacji Oprócz samouczenia się, system musi wykorzystywać inne metody analizy zaszyfrowanej komunikacji, co najmniej TLS fingerprinting i związane z tym wykrywanie znanych zagrożeń.
29. Aktualizacje systemu i sygnatur, w tym tryb offline	
5. Aktualizacje a. Komponentów oprogramowania narzędziowego odbywają się manualnie i realizuje je administrator rozwiązania	6. Aktualizacje systemu muszą być możliwe do przeprowadzenia przez użytkownika w trybie offline. 2. Bazy danych muszą być aktualizowane co najmniej raz na godzinę. Nie mogą to być tylko darmowe/otwarte bazy danych, ale muszą to być komercyjne bazy danych

NDR Specyfikacja równoważna	NDR Specyfikacja Obecna
b. Sygnatur realizowane są i. online – w sposób automatyczny ii. manualnie – poprzez pobranie paczki aktualizacyjnej i przesłanie jej do oprogramowania narzędziowego przy użycia nośnika przenośnego; iii. lokalnie – przy użyciu lokalnego repozytorium	dostarczone przez producenta rozwiazania w ramach dedykowanej licencji.
30. Zarządzanie danymi, retencja i logi	
6. Zarządzanie danymi a. backup – pozwala na tworzenie i przywracanie kopii zapasowych stworzonych konfiguracji rozwiązania; b. retencja danych – dane przechowywane są na urządzeniu administrującym, przez ograniczony czas, który może być uzależniony od: i. zajętości pamięci ii. ręcznie ustawionego czasu retencji danych; c. logi systemowe – system musi umożliwiać tworzenie i archiwizowanie logów systemowych oraz supportowych logów systemowych; d. usuwanie danych – system musi	Przetwarzanie i przechowywanie przepływów sieciowych 1. System przechowuje przepływy sieciowe w formacie umożliwiającym analizę komunikacji sieciowej na poziomie poszczególnych przepływów, w tym śledzenie informacji o transakcjach aplikacji i ich metadanych od L2 do L7 zawartych w danym przepływie sieciowym. 2. Wymagane protokoły do przechowywania metadanych aplikacji z poszczególnych transakcji to DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, enkapsulacja SSL/TLS. 3. System musi być w stanie zbierać i analizować dzienniki aplikacji i systemu w formacie co najmniej syslog z monitorowanych urządzeń oraz identyfikować niebezpieczne lub potencjalnie szkodliwe działania.

mieć możliwość usuwania danych z możliwością wyboru, których typów danych ta akcja dotyczy.	
31. Licencjonowanie	
3. Licencja na zakup i serwis oprogramowania bazuje na ilości aktywnie występujących w ruchu sieciowym adresów IP.	Licencja 1. Bezterminowe licencje na oprogramowanie wraz z 12-miesięcznym okresem wsparcia muszą być zapewnione dla wszystkich dostarczonych komponentów oprogramowania. Subskrypcja SW nie będzie akceptowana.

Przedłużenie terminu składania ofert
W związku z dokonaną zmianą treści SWZ/OPZ, polegającą na dopuszczeniu rozwiązań równoważnych w zakresie XDR oraz NDR, Zamawiający, działając na podstawie art. 286 ust. 3 ustawy Pzp, przedłuża termin składania ofert w celu zapewnienia Wykonawcom czasu niezbędnego do zapoznania się z wprowadzonymi zmianami oraz ich uwzględnienia przy przygotowaniu ofert.
Nowy termin składania ofert: 14.08.2026 r. do godz. 9:00, termin otwarcia 14.08.2026 r. godz. 9:15.
W związku z powyższym odpowiedniej zmianie ulega termin składania i otwarcia ofert wskazany w SWZ oraz w ogłoszeniu o zamówieniu.
Zamawiający dokona stosownej zmiany ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych.
Pozostałe postanowienia SWZ i OPZ pozostają bez zmian.