Załącznik nr 1 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

System antywirusowy wraz z ochroną EDR dla wszystkich stanowisk

LP	Wymagania minimalne
I.	**Przedmiot zamówienia**
1	Przedmiotem zamówienia jest wdrożenie systemu antywirusowego wraz z funkcjonalnością EDR (Endpoint Detection and Response). System ten jest niezbędny dla zapewnienia skutecznej ochrony punktów końcowych Szpitala.
2	Stosowany obecnie klasyczny system antywirusowy, mimo ważnej licencji do czerwca 2026r. nie zapewnia mechanizmów, które gwarantują bezpieczeństwo systemów w Szpitalu w wystarczającym zakresie.
3	Ilość wymaganych licencji na stanowiska robocze: 1100
4	Ilość wymaganych licencji serwerowych: 10
5	Rozwiązanie musi zapewniać wsparcie dla około 2000 kont w Active Directory
6	Wdrożenie ma na celu zapewnienie ciągłości działania infrastruktury, zostanie przeprowadzone w odpowiednich etapach, uwzględniając dobre praktyki i zalecenia producenta.
II.	**Wymagania dotyczące wdrożenia**
1	Wdrożenie ma na celu zwiększenie bezpieczeństwa infrastruktury, dzięki zastosowaniu nowoczesnego rozwiązania klasy XDR. Konsola zarządzająca rozwiązania występuje w formie SaaS i jest udostępniana przez producenta.
2	Wdrożenie zostanie przeprowadzone w formie sesji zdalnych, z udziałem inżynierów Zamawiającego. Prace będą wykonywane w dni robocze, od poniedziałku do piątku, w godzinach 8-14, z wyłączeniem świąt i dni ustawowo wolnych od pracy.
3	Wykonawca przygotuje paczki instalacyjne agentów w formatach exe/msi, dostosowane do mechanizmów dystrybucji i instalacji oprogramowania stosowanych przez Zamawiającego, wraz z niezbędną dokumentacją techniczną.
4	Instalacja agentów w środowisku oraz ewentualna deinstalacja obecnie używanego oprogramowania realizowana będzie przez Zamawiającego. Rola Wykonawcy ogranicza się do wsparcia technicznego i przygotowania materiałów instalacyjnych.
5	Wykonawca przygotuje projekt wdrożenia systemu XDR w formie dokumentu HLD (High Level Design), obejmującego architekturę rozwiązania, sposób integracji z infrastrukturą Zamawiającego oraz harmonogram wdrożenia.
6	Dokument HLD podlega akceptacji Zamawiającego, a rozpoczęcie wdrożenia możliwe jest wyłącznie po jej uzyskaniu.
7	Wdrożenie systemu XDR zostanie zrealizowane zgodnie z zaakceptowanym HLD. Wszelkie zmiany wymagają uprzedniej zgody Zamawiającego.
8	Wykonawca opracuje i przeprowadzi testy akceptacyjne potwierdzające poprawność wdrożenia i zgodność z wymaganiami Zamawiającego oraz HLD. Testy realizowane są z udziałem Zamawiającego o kończą się raportem z testów akceptacyjnych podlegającym zatwierdzeniu.
9	Po zakończeniu wdrożenia Wykonawca dostarczy dokumentację powykonawczą, obejmującą opis wdrożonego rozwiązania. Dokumentacja podlega akceptacji Zamawiającego.
10	Wykonawca zapewni przeprowadzenie instruktażu z zakresu obsługi i administracji systemu XDR w formie warsztatowej. Instruktaż zostanie przeprowadzony w języku polskim i będzie obejmowało autorskie materiały w języku polskim.
11	Czas trwania instruktażu nie może być krótszy niż 2 dni po minimum 6h. Dopuszcza się realizację w formie zdalnej.
12	Instruktaż przeznaczony będzie dla maksymalnie 5 użytkowników ze strony Zamawiającego.
13	Na czas trwania instruktażu, Wykonawca udostępni uczestnikom dedykowane środowisko szkoleniowe umożliwiające wykonywanie
III.	**Wsparcie powdrożeniowe.**
1	Wykonawca zapewni wsparcie techniczne w wymiarze 3 godzin miesięcznie (łącznie 108 godzin w okresie obowiązywania umowy), przy czym niewykorzystane godziny wsparcia w danym miesiącu nie przechodzą na kolejne miesiące, nie podlegają kumulacji ani rozliczeniu w innym okresie.

2	Wsparcie techniczne realizowane będzie przez certyfikowanych inżynierów wykonawcy, posiadających odpowiednie kwalifikacje w zakresie oferowanych rozwiązań.
3	Zakres wsparcia obejmuje pomoc w konfiguracji, parametryzacji oraz bieżącym utrzymaniu wspieranych rozwiązań.
4	Wykonawca zapewni rozwiązywanie zgłoszonych problemów, konsultacje techniczne oraz bieżącą pomoc w ramach realizowanych zgłoszeń serwisowych.
5	Wykonawca będzie cyklicznie, nie rzadziej niż raz na kwartał, przedstawiał Zamawiającemu propozycje optymalizacji wykorzystania dostarczonych rozwiązań.
6	Wsparcie obejmuje udział Wykonawcy w okresowych spotkaniach prewencyjnych realizowanych na żądanie Zamawiającego, w celu omówienia bieżących działań i stanu środowiska.
7	Wykonawca zapewni pośrednictwo w kontaktach z producentem oferowanego rozwiązania.
8	Wykonawca zapewni dostęp do systemu obsługi zgłoszeń przez cały okres obowiązywania umowy, umożliwiającego rejestrowanie zgłoszeń serwisowych, przy czym wszystkie działania realizowane w ramach wsparcia technicznego muszą być ewidencjonowane w tym systemie. Rozwiązanie musi być udostępnione na zasobach Wykonawcy.
IV.	**Specyfikacja wymagań systemowych**
1	Agent musi obsługiwać funkcjonalności Next Generation EPP (Endpoint Protection Platform) oraz EDR (Endpoint Detection and Response) w jednym autonomicznym agencie, który do realizacji swoich funkcjonalności nie potrzebuje łączności z chmurą lub konsolą zarządzającą. Wymagane jest wsparcie dla systemów operacyjnych Windows, macOS i Linux.
2	Rozwiązanie musi umożliwiać identyfikację zaawansowanych zagrożeń, w szczególności ataków bezplikowych, złośliwego oprogramowania typu 0-day oraz nadużyć polegających na wykorzystywaniu podatności posiadanego oprogramowania lub sprzętu, niezależnie od mechanizmów detekcji opartych na sygnaturach lub reputacji. Przez silniki reputacji Zamawiający rozumie mechanizmy identyfikacji zagrożeń oparte na reputacji takich elementów jak: adresy IP, rekordy DNS, adresy URL oraz skróty/hashe plików.
3	Agent musi być w pełni autonomiczny, co oznacza, że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani ŻADNYCH zasobów zewnętrznych od agenta. Wykrywanie i reagowanie na zaawansowane zagrożenia (0-day, bezplikowe, oparte na pamięci RAM, Exploity 0-Day, ransomware, cryptominers, lateral movement, APT) musi być możliwe w czasie rzeczywistym, nie może zależeć od stanu sieciowego stacji (agent musi realizować te same funkcjonalności w trybie online i offline) oraz nie może wymagać innego rodzaju zewnętrznych zasobów.
4	Informacje na temat incydentów bezpieczeństwa muszą być przechowywane co najmniej przez 365 dni.
5	Rozwiązanie musi zapewniać możliwość konfiguracji polityk bezpieczeństwa na następujących poziomach: a) Poziomie Grupy Komputerów. b) Poziomie Lokalizacji gromadzącej Grupy Komputerów. c) Poziomie Konta gromadzącym Lokalizacje. d) Polityki bezpieczeństwa muszą być automatycznie dziedziczone z wyższych poziomów hierarchii przez niższe poziomy (Konto -> Lokalizacja -> Grupa Komputerów).
6	Rozwiązanie musi pozwalać na złamanie dziedziczenia na dowolnym poziomie tak, aby można było zmodyfikować politykę bezpieczeństwa. Zmodyfikowana polityka bezpieczeństwa musi być automatycznie dziedziczona przez niższe poziomy hierarchii.
7	Rozwiązanie musi wykrywać zagrożenia rozróżniając dwa poziomy incydentów: podejrzane i złośliwe.
8	Rozwiązanie musi pozwalać na skonfigurowanie automatycznych akcji odpowiedzi na zaistniały incydent takich jak: a) Generowanie alarmu b) Zabicie procesu/procesów należących do tego samego incydentu c) Przeniesienie do kwarantanny złośliwych plików należących do tego samego incydentu. Funkcja kwarantanny musi zatrzymać procesy, szyfrować plik wykonywalny i przenieść go na ograniczoną ścieżkę. d) Wykonanie naprawy (tylko dla systemów Windows i MacOS). Funkcja naprawy musi zatrzymać procesy, poddać kwarantannie pliki binarne, usunąć połączone biblioteki,

	usunąć pliki źródłowe i przywrócić konfigurację systemu operacyjnego, aplikacji i ustawień użytkownika do stanu sprzed rozpoczęcia ataku. e) Wykonanie operacji rollback (tylko dla systemów Windows). Funkcja Rollback musi przywracać stan stacji końcowej do stanu z momentu utworzenia migawki VSS (Volume Shadow Copy), cofając zmiany wprowadzone przez złośliwy proces i skojarzone z nim zasoby. Agent powinien autonomicznie i w czasie zbliżonym do rzeczywistego przywrócić dane z chronionego hosta w przypadku ataku z wykorzystaniem szkodliwego oprogramowania typu ransomware. f) Wykonanie operacji izolacji sieciowej stacji końcowej na której wydarzył się incydent. Funkcja izolacji sieciowej musi pozwalać na komunikację agenta z konsolą zarządzającą. Stacja końcowa nie może komunikować się z innymi elementami w sieci. Wszystkie działania na konsoli zarządzania muszą działać niezależnie od stanu izolacji sieci agenta.
9	Rozwiązanie musi być wyposażone w zestaw silników które można włączać lub wyłączać.
10	Silnik detekcji muszą wykrywać zagrożenia co najmniej w następującym zakresie: a) Reputacja. b) Analiza statyczna struktury plików. c) Analiza behawioralna uruchomionych procesów. d) Analiza dokumentów i skryptów. e) Wykrywanie ruchów poziomych. f) Wykrywanie prób exploitacji systemu operacyjnego. g) Wykrywanie ataków bezplikowych. h) Wykrywanie potencjalnie niepożądanych aplikacji. i) Wykrywanie ataków interaktywnych generowanych z poziomu CMD lub Powershell.
11	Rozwiązanie musi zapewniać silny mechanizm „Anti-Tamper”, czyli mechanizmy ochrony przed manipulacja oprogramowaniem przez malware lub użytkownika końcowego. Taki mechanizm musi być chroniony unikalnym hasłem dla każdego komputera końcowego. Stan WŁ./WYŁ. ochronę przed manipulacją musi być opcją konfigurowalną w polityce bezpieczeństwa.
12	Rozwiązanie musi zapewniać możliwość konfiguracji automatycznego skanowania nowo zainstalowanych agentów.
13	Rozwiązanie musi zapewniać możliwość konfiguracji (włączenia/wyłączenia) logowania zachowania agenta na stacji końcowej.
14	Rozwiązanie musi zapewniać możliwość konfiguracji widoczności agenta i informacji wyświetlanych użytkownikowi na stacji końcowej.
15	Rozwiązanie musi zapewniać możliwość włączenie lub wyłączenia mechanizmu zbierania metadanych EDR dla wybranych komputerów.
16	Rozwiązanie musi zapewniać możliwość szczegółowej konfiguracji zbieranych metadanych EDR. Musi istnieć możliwość włączenia/wyłączenia zbierania informacji co najmniej o: a) Stworzonych procesach. b) Plikach (tworzenie, kasowanie, modyfikowanie, skanowanie, zmiana nazwy). c) Odwiedzanych URL-ach. d) Zapytaniach DNS-owych. e) Komunikacji IP. f) Operacjach logowania i wylogowania ze stacji końcowej. g) Operacjach na kluczach rejestru Windows (tworzenie, importowanie, kasowanie, zmienia nazwy, eksportowanie). h) Operacji na wartościach rejestru Windows (tworzenie, kasowanie, modyfikowanie). i) Operacje menadżera zadań Windows (start zadania, kasowanie zadania, aktualizacja zadania, rejestrowanie zadania, wyzwolenie zadania). j) Indykatorach zachowań. k) Ładowania bibliotek dll. l) Komendach skryptów. m) Komunikacji między procesami. n) Wgranych sterownikach. o) Operacjach na nazwanych łączach (tworzenie, dołączanie).
17	Rozwiązanie musi zapewniać możliwość ukrywania (maskowania) ścieżek i nazw plików dla formatów zip, pdf, ms-office.

18	Rozwiązanie musi zapewniać możliwość konfiguracji automatycznego pobierania złośliwych plików wykrytych w incydencie bezpieczeństwa.
19	Rozwiązanie musi zapewniać możliwość definiowania przedziału czasu (w dniach) po jakim nieaktywna stacja końcowa powinna zwalniać licencję.
20	Rozwiązanie musi zapewniać możliwość włączenia/wyłączenia funkcji zdalnego dostępu do wybranej grupy stacji końcowych.
21	Rozwiązanie musi posiadać strukturę pozwalającą na podział środowiska na konto, lokalizacje i grupy, aby ułatwić zarządzanie oraz kontrolę dostępu do środowiska.
22	Struktura rozwiązania musi wyszczególniać następujące poziomy: a) Globalny - poziom agregujący utrzymywany przez dostawcę rozwiązania. b) Konto - Podstawowy poziom struktury rozwiązania dla użytkownika (klienta) końcowego konsoli zarządzającej oferowanego rozwiązania. Każde Konto może agregować wiele lokalizacji. Konto może mieć zdefiniowane własne reguły i polityki, jak również dziedziczyć je z poziomu globalnego. c) Lokalizacja - segment struktury rozwiązania agregowany pod poziomem konta. Każda lokalizacja może posiadać własne reguły i ustawienia i/lub dziedziczyć ustawienia globalne lub z konta. Lokalizacja może należeć tylko do jednego Konta. d) Grupa - segment struktury rozwiązania agregowany pod poziomem lokalizacji. Każda grupa może posiadać własne ustawienia i/lub dziedziczyć ustawienia globalne, konta lub lokalizacji. Grupa może należeć tylko do jednej Lokalizacji.
23	Rozwiązanie musi posiadać panel struktury, pozwalający przechodzić między zakresami w konsoli zarządzania.
24	Każda lokalizacja musi pozwalać na przypisywanie licencji z puli przypisanej do konta pod którą się znajduję.
25	Każda lokalizacja musi pozwalać na zdefiniowanie parametru czasu ważności lokalizacji, po którym przypisane do niego licencje zostaną zwolnione.
26	Każde Konto, Lokalizacja i Grupa muszą mieć własną politykę lub dziedziczyć politykę od wyższych poziomów hierarchii.
27	Dziedziczenie polityk musi działać domyślnie dla Konta, Lokalizacji i Grup, do momentu zdefiniowania przez użytkownika zmiany w polityce dla instancji na swoim poziomie dostępu.
28	Grupy, Lokalizacje, Konta i Globalne mogą definiować swoje własne wpisy w ramach listy wykluczeń i listy blokowania.
29	Każdy poziom struktury rozwiązania musi dziedziczyć listę wykluczeń i listy blokowania od wyższych poziomów hierarchii.
30	Grupy, Lokalizacje, Konta i Globalne mogą definiować swoje własne wpisy w ramach modułów kontroli sieci oraz kontroli urządzeń.
31	Dziedziczenie reguł w ramach modułów kontroli sieci oraz kontroli urządzeń musi być opcjonalne i konfigurowalne przez administratora.
32	Rozwiązanie musi mieć możliwość filtrowania stacji końcowych na których został zainstalowanych agent, co najmniej z wykorzystaniem następujących parametrów: a) Nazwa stacji końcowej. b) Tag przypisany do stacji końcowej. c) System operacyjny stacji końcowej. d) Wersja zainstalowanego agenta. e) Typ stacji końcowej: a. Laptop. b. Desktop. c. Serwer. d. Host Kubernetes. e. Storage. f. Inny. f) Domena MS Windows. g) Czy agent połączony jest do konsoli zarządzania. h) Stan zdrowia agenta. i) Stan sieci stacji końcowej. j) Czy było wykonane pełne skanowanie dysku.

	k) Czy agent oczekuje na aktualizacje. l) Architekturę systemu operacyjnego. m) Szyfrowanie dysku. n) Status podatności. o) Rodzaj użytego instalatora. p) Lokacja. q) Stan firewalla. r) Stan operacyjny. s) Jakikolwiek ciąg znaków z domeny Microsoft Windows. t) MAC adres. u) Lokalny adres IP. v) Numer seryjny stacji końcowej.
33	Rozwiązanie musi mieć możliwość zapisywania skonfigurowanych filtrów w celu ich późniejszego wykorzystania.
34	Rozwiązanie musi mieć możliwość użycia zapisanych filtrów do tworzenia dynamicznych grup stacji końcowych.
35	Rozwiązanie musi mieć możliwość dodawania wyjątków ograniczających działanie agenta dla wybranych aplikacji celem zapewnienia zgodności.
36	Rozwiązanie musi umożliwiać tworzenie wyjątków dla systemu Microsoft Windows z wykorzystaniem następujących elementów: a) HASH SHA1. b) Ścieżka do pliku. c) Ścieżka do katalogu wraz z katalogami podrzędnymi. d) Certyfikat. e) Rodzaj pliku. f) Przeglądarka.
37	Rozwiązanie musi umożliwiać tworzenie wyjątków dla systemu Linux z wykorzystaniem następujących elementów: a) HASH SHA1. b) Ścieżka do pliku. c) Ścieżka do katalogu wraz z katalogami podrzędnymi. d) Certyfikat.
38	Rozwiązanie musi umożliwiać tworzenie wyjątków dla systemu MacOS z wykorzystaniem następujących elementów: a) HASH SHA1. b) Ścieżka do pliku. c) Ścieżka do katalogu wraz z katalogami podrzędnymi. d) Certyfikat.
39	Rozwiązanie, dla wyjątków typu "Ścieżka" w systemie Windows musi mieć możliwość stopniowania poziomu wyjątków, co najmniej w następującym zakresie: a) Wygaszenie alarmów. b) Wyłączenie monitorowania konkretnego procesu. c) Wyłączenie monitorowania konkretnego procesu i jego procesów potomnych.
40	Rozwiązanie, dla wyjątków typu "Ścieżka" w systemie MacOS musi mieć możliwość stopniowania poziomu wyjątków, co najmniej w następującym zakresie: a) Wygaszenie alarmów. b) Zredukowanie monitorowania konkretnego procesu. c) Zredukowanie monitorowania konkretnego procesu i jego procesów potomnych. d) Wyłączenie monitorowania konkretnego procesu. e) Wyłączenie monitorowania konkretnego procesu i jego procesów potomnych.
41	Rozwiązanie musi posiadać gotowy katalog wyjątków przygotowany dla wybranych aplikacji i aktualizowany przez producenta.
42	Rozwiązanie musi posiadać możliwość konfigurowania wyjątków na różnych poziomach hierarchii z zachowaniem zasad dziedziczenia z wyższych poziomów do niższych.
43	Rozwiązanie musi mieć możliwość tworzenia list blokujących z wykorzystaniem funkcji skrótu SHA1 dla następujących systemów operacyjnych:

	a) Microsoft Windows. b) Linux. c) MacOS.
44	Rozwiązanie musi posiadać możliwość konfigurowania list blokujących na różnych poziomach hierarchii z zachowaniem zasad dziedziczenia z wyższych poziomów do niższych.
45	Rozwiązanie musi być wyposażone w moduł kontroli sieci IP, który umożliwi kontrolowanie lokalnego firewalla stacji końcowych.
46	Rozwiązanie musi oferować zunifikowane reguły dla dowolnego systemu operacyjnego, co oznacza, że musi umożliwiać przypisywanie reguł do jednego lub wielu systemów operacyjnych.
47	Moduł kontroli sieci musi być zintegrowany z funkcjonalnością tagowania hostów w oferowanym rozwiązaniu. Moduł kontroli sieci musi być zintegrowany z strukturą konsoli zarządzającej i pozwalać na zarządzanie regułami w obrębie poszczególnych poziomów struktury.
48	Moduł kontroli sieci musi pozwalać na tworzenie dwóch typów reguł firewall: a) Blokowanie ruchu. b) Dopuszczanie ruchu.
49	Moduł kontroli sieci musi umożliwiać definiowane reguł przez następujące parametry: a) Protokół
50	Moduł kontroli sieci musi definiować minimum 139 reguł, które będą możliwe do zdefiniowania reguły: a) Aplikacja. b) Dowolna aplikacja. c) Ścieżka aplikacji. d) Kierunek transmisji. e) Przychodzący. f) Wychodzący. g) Lokalny host. h) Każdy host. i) Adres IP. j) CIDR. k) Zakres adresacji IP. l) Lokalny port. m) Dowolny port. n) Numer portu. o) Zakres portów. p) Zdalny host. q) Każdy host. r) Adres IP. s) FQDN. t) Zakres adresacji IP. u) Zdalny port. v) Numer portu. w) Zakres portów. x) Lokalizacja hosta.
51	Moduł kontroli sieci musi oferować możliwość filtrowania reguł firewall w następujących kategoriach: a) Poziomami struktury rozwiązania dla których reguły są aplikowane. b) System operacyjny. c) Status (włączona / wyłączona). d) Akcja (zezwalaj / blokuj). e) Kierunek transmisji.
52	Moduł kontroli sieci musi oferować możliwość wyszukiwania reguł poprzez tekst w oparciu o: a) Nazwę aplikacji. b) Nazwę reguły. c) Usługę. d) Tag.

	Moduł kontroli sieci musi oferować możliwość włączenia lub wyłączenia funkcjonalności firewall.
53	Moduł kontroli sieci musi oferować tryb dziedziczenia reguł w ramach struktury rozwiązania: a) Brak dziedziczenia. b) Automatyczne dziedziczenie reguł z wyższych poziomów struktury rozwiązania. c) Manualne dziedziczenie, oparte na mechanizmie tagowania hostów.
54	Interfejs graficzny modułu kontroli sieci musi prezentować reguły w formie tabularycznej, z możliwością definiowania następujących kolumn: a) Nazwę. b) Opis. c) Aplikacja. d) Tag. e) Poziomami struktury rozwiązania, dla których reguły są aplikowane. f) System operacyjny. g) Status (włączona / wyłączona). h) Akcja (zezwalaj / blokuj). i) Kierunek transmisji. j) Lokalny host. k) Lokalny port. l) Zdalny host. m) Zdalny port. n) Lokalizacja hosta.
55	Interfejs graficzny modułu kontroli sieci musi oferować możliwość eksportowania wybranych reguł do pliku .json.
56	Interfejs graficzny modułu kontroli sieci musi oferować możliwość importowania wybranych reguł z pliku .json.
57	Moduł kontroli sieci nie może definiować automatycznych domyślnych reguł. Ruch musi być zezwolony, jeśli nie zostanie on zablokowany przez regułę dodaną przez administratora.
58	Włączenie ochrony firewall w module kontroli sieci powoduje, że staje się on aktywnym firewallem w systemie Windows. Firewall z modułu sieci przejmuje kontrolę nad ruchem IP hosta, ale nie zmienia reguł innych rozwiązań firewall na danym systemie.
59	Reguły firewalla systemu Windows oraz reguły firewalla GPO muszą stać się automatycznie nieaktywne po włączeniu firewalla w module kontroli sieci rozwiązania.
60	Moduł kontroli sieci z włączonym firewall nie może być zarejestrowany jako firewall w systemie Linux. Firewall rozwiązania musi działać równolegle do firewalla systemowego systemu Linux. W przypadku konfliktu między firewallami systemowym a rozwiązania, zasady firewalla rozwiązania muszą traktowane być priorytetowo.
61	Moduł kontroli sieci w przypadku firewalla na systemach macOS (w wersjach Big Sur i nowszych) musi opierać się na interfejsie Network Extension dostarczonym przez firmę Apple i wykorzystywać filtr treści do implementacji funkcji firewall.
62	Funkcja firewall dla macOS musi umożliwiać stosowanie reguł dla protokołów TCP i UDP. Inne protokoły sieciowe nie są wymagane dla agenta macOS.
63	Reguły firewall muszą być wykonywane według kolejności ustalonej przez administratora. Administrator z dostępem do edycji moduł kontroli sieci musi mieć możliwość zmiany kolejność reguł w zakresie poziomów struktury rozwiązania, którymi zarządza.
64	Moduł kontroli sieci musi być zintegrowany z funkcjonalnością kwarantanny sieciowej hostów w oferowanym rozwiązaniu.
65	Moduł kontroli sieci musi umożliwiać definiowanie wyjątków dla funkcjonalności kwarantanny sieciowej hostów w oferowanym rozwiązaniu.
66	Tworzenie wyjątków dla kwarantanny sieciowej hostów musi oferować te same parametry co reguły firewall oferowanego rozwiązania.
67	Wyjątki dla kwarantanny sieciowej hostów muszą być prezentowane w tej samej formie co reguły firewall rozwiązania.
68	Wyjątki dla kwarantanny sieciowej hostów muszą umożliwiać filtrowanie wyjątków, jak w przypadku reguły firewall rozwiązania.
69	Moduł kontroli sieci musi oferować możliwość włączenia lub wyłączenia wyjątków dla kwarantanny sieciowej rozwiązania.

70	Moduł kontroli sieci musi oferować tryb dziedziczenia wyjątków dla kwarantanny sieciowej rozwiązania takie jak: a) Brak dziedziczenia. b) Automatyczne dziedziczenie reguł z wyższych poziomów struktury rozwiązania. c) Manualne dziedziczenie, oparte na mechanizmie tagowania hostów.
71	Interfejs graficzny modułu kontroli sieci musi oferować możliwość eksportowania wybranych wyjątków dla kwarantanny sieciowej rozwiązania do pliku .json.
72	Interfejs graficzny modułu kontroli sieci musi oferować możliwość importowania wybranych wyjątków dla kwarantanny sieciowej rozwiązania z pliku .json.
73	Rozwiązanie musi mieć funkcjonalność kontroli urządzeń podłączanych do stacji końcowej za pomocą następujących interfejsów: a) Bluetooth. b) USB.
74	Reguły kontrolne dla interfejsu Bluetooth muszą mieć możliwość wybrania jako parametru klasyfikującego co najmniej: a) Identyfikatora sprzętowego urządzenia. b) Wersji protokołu Bluetooth.
75	Reguły kontrolne dla interfejsu Bluetooth, przy wybrani opcji identyfikatora sprzętowego urządzenia muszą pozwalać na określenie: a) Numeru ID producenta urządzenia. b) Numeru ID konkretnego urządzenia. c) Klasy głównej urządzenia. d) Klasy podrzędnej urządzenia.
76	Reguły kontrolne dla interfejsu USB muszą mieć możliwość wybrania jako parametru klasyfikującego co najmniej: a) Numeru ID producenta urządzenia. b) Klasy urządzenia. c) Numeru seryjnego urządzenia. d) Numeru ID konkretnego urządzenia.
77	Funkcjonalność kontroli urządzeń musi być obsługiwana dla następujących systemów operacyjnych: a) Microsoft Windows. b) MacOS.
78	Rozwiązanie musi posiadać możliwość konfigurowania reguł kontroli urządzeń na różnych poziomach hierarchii z zachowaniem zasad dziedziczenia z wyższych poziomów do niższych.
79	Rozwiązanie musi mieć możliwość wykonania Full Remote Shell, aby administrator mógł wykonywać polecenia na stacji końcowej, nawet gdy jest ona w stanie izolacji sieciowej.
80	Funkcjonalność Full Remote Shell musi być dostępna dla następujących systemów operacyjnych i środowisk: a) Microsoft Windows. b) MacOS. c) Linux. d) Kubernetes.
81	Dostęp do powłoki zdalnej powinien wymuszać na Administratorze uwierzytelnianie dwuskładnikowe (2FA) w celu udzielenia dostępu.
82	Rozwiązanie musi zapisać transkrypcję zestawionej sesji.
83	Transkrypcja sesji zdalnej musi być chroniona hasłem.
84	Rozwiązanie musi mieć możliwość skonfigurowania dostępności funkcji Full Remote Shell w politykach bezpieczeństwa.
85	Rozwiązanie musi mieć możliwość mapowania wskaźników zagrożenia znalezionych w incydentach bezpieczeństwa do odpowiednich technik frameworku MITRE ATT&CK.
86	Rozwiązanie musi pozwalać na wykonywanie zapytań EDR/XDR z wykorzystaniem elementów frameworku MITRE ATT&CK, co najmniej takich jak: a) Numer techniki. b) Nazwa taktyki.

87	Rozwiązanie musi posiadać tabelę wizualizującą wszystkie techniki frameworku MITRE ATT&CK wspierane przez system.
88	Rozwiązanie musi posiadać możliwość budowania reguł detekcyjnych z wykorzystaniem frameworku MITRE ATT&CK, co najmniej takich jak: a) Numer techniki. b) Nazwa taktyki.
89	Rozwiązanie musi posiadać dokumentację co najmniej w języku angielskim wbudowaną w konsolę do zarządzania.
90	Dokumentacja powinna być dostępna po zalogowaniu się do konsoli do zarządzania.
91	Rozwiązanie w panelu konfiguracyjnym polityk bezpieczeństwa, musi posiadać podpowiedzi wbudowane w konsolę pomagające zrozumieć dostępne opcje.
92	Rozwiązanie musi posiadać moduł tworzenia raportów.
93	Moduł tworzenia raportów musi oferować predefiniowane wzorce zawartości raportów.
94	Moduł tworzenia raportów musi oferować możliwość tworzenia raportu na żądanie.
95	Moduł tworzenia raportów musi oferować możliwość automatycznego tworzenia raportów w oparciu o harmonogram.
96	Zakres czasu raportów musi być możliwy do zdefiniowania przez użytkownika konsoli zarządzającej.
97	Wygenerowane raporty muszą być przechowywane w konsoli zarządzającej do momentu skasowania ich przez użytkownika konsoli oraz muszą być dostępne do pobrania w formacie PDF oraz HTML.
98	Rozwiązanie musi mieć możliwość wyświetlania zaistniałych incydentów bezpieczeństwa do 365 dni wstecz.
99	Rozwiązanie musi mieć możliwość filtrowania wyświetlanych incydentów za pomocą co najmniej następujących parametrów: a) Status mitygacji zagrożenia. b) Poziom incydentu. c) Wybrany tag. d) Status incydentu. e) Czy potrzebny jest restart stacji końcowej. f) System operacyjny. g) Wersja systemu operacyjnego. h) Silnik, który wykrył zagrożenie. i) Klasyfikacja zagrożenia. j) Co zainicjowało wykrycie zagrożenia. k) Czy agent na stacji końcowej jest w trybie online. l) Czy istnieje notatka przypisana do incydentu. m) Czy istnieje zgłoszenie konkretnego incydentu w zewnętrznym systemie.
100	Rozwiązanie musi mieć możliwość wyświetlania alarmów wygenerowanych przez własnoręcznie tworzone reguły detekcyjne.
101	Rozwiązanie musi mieć możliwość filtrowania wyświetlanych alarmów za pomocą co najmniej następujących parametrów: a) Nazwa stacji końcowej. b) Nazwa procesu. c) Nazwa reguły detekcyjnej. d) Funkcja skrótu SHA1. e) Funkcja skrótu SHA256. f) Funkcja skrótu MD5. g) Ścieżka. h) Werdykt analityka. i) Status incydentu. j) Rodzaj stacji końcowej (desktop, laptop, serwer, itp.). k) System operacyjny stacji końcowej. l) Poziom Severity.
102	Rozwiązanie musi mieć możliwość automatycznej aktualizacji agentów zainstalowanych na stacjach końcowych z systemem operacyjnym:

	a) Microsoft Windows. b) Linux. c) MacOS.
103	Funkcjonalność automatycznej aktualizacji musi pozwalać na wybór wersji agenta do jakiej należy wykonać aktualizację.
104	Funkcjonalność automatycznej aktualizacji musi pozwalać na wybór czasu, w którym aktualizacja powinna zostać wykonana posiadając możliwość wyboru co najmniej: a) Natychmiastowej aktualizacji. b) Aktualizacji zgodnej ze zdefiniowanym oknem aktualizacyjnym.
105	Funkcjonalność automatycznej aktualizacji musi pozwalać na wybór stacji końcowych które powinny zostać zaktualizowane posiadając możliwość wyboru co najmniej: a) Wszystkich stacji końcowych na wybranym poziomie hierarchii. b) Jedynie stacji końcowych z wybranym tag-iem.
106	Rozwiązanie musi posiadać możliwość konfigurowania funkcjonalność automatycznej aktualizacji agentów na różnych poziomach hierarchii z zachowaniem zasad dziedziczenia z wyższych poziomów do niższych i możliwością przerwania dziedziczenia na dowolnym poziomie hierarchii.
107	Rozwiązanie musi mieć możliwość definiowania okna aktualizacyjnego w którym będzie możliwość wykonania aktualizacji agentów zainstalowanych na stacjach końcowych.
108	Rozwiązanie musi mieć możliwość zdefiniowania maksymalnej liczby stacji końcowych pobierających jednocześnie paczkę aktualizacyjną.
109	Rozwiązanie musi automatycznie wykrywać stacje końcowe w sieci bez konieczności wdrażania dodatkowych czujników, snifferów lub innego tego typu sprzętu na których nie został zainstalowany agent.
110	Rozwiązanie musi wykrywać co najmniej następujące urządzenia: a) Microsoft Windows. b) Linux. c) Apple. d) Windows Legacy.
111	Dla wykrytych urządzenie rozwiązanie musi wyświetlać następujące informacje: a) Producent. b) System operacyjny. c) Funkcja urządzenia. d) Wersja systemu operacyjnego. e) Adres MAC. f) Adres IP. g) Nazwa hosta. h) Kiedy urządzenie było widziane po raz pierwszy. i) Kiedy informacje o urządzeniu zostały zaktualizowane.
112	Rozwiązanie musi mieć możliwość pobrania paczki instalacyjnej bezpośrednio z konsoli do zarządzania.
113	Rozwiązanie musi posiadać instalator dla: a) Microsoft Windows. b) MacOS. c) Linux.
114	Dla systemu operacyjnego Microsoft Windows rozwiązanie musi posiadać instalator w następujących formatach: a) MSI 32 bit. b) MSI 64 bit. c) EXE 32 bit. d) EXE 64 bit.
115	Dla systemu operacyjnego MacOS rozwiązanie musi posiadać instalator w formacie PKG.
116	Dla systemu operacyjnego Linux rozwiązanie musi posiadać instalator w formacie: a) RPM x86 64 bit. b) DEB x86 64 bit. c) RPM AArch 64 bit d) DEB AArch 64 bit.

116	Dla systemu Kubernetes rozwiązanie musi posiadać instalator w formacie GZ.
117	Rozwiązanie musi posiadać możliwość łatwego filtrowania dostępnych pakietów instalacyjnych.
118	Dla każdego pakietu instalacyjnego muszą być podane co najmniej następujące informacje: a) Poziom dostępności (EA, GA). b) Wersja główna. c) Numer buildu. d) Rozszerzenie pliku. e) Nazwa pliku. f) Wielkość pliku. g) Data opublikowania. h) Wartość SHA1. i) Platforma.
119	Rozwiązanie musi zapewniać narzędzia pozwalające na analizę i przeszukiwanie zebranych metadanych EDR.
120	Dostarczone narzędzie musi posiadać przykładowe, gotowe zapytania EDR pozwalające na wyświetlenie co najmniej następujących informacji: a) Zdarzenia wygenerowane przez stacje końcowe w ostatniej godzinie. b) Wszystkie aktywności w rejestrze Windows dla wszystkich stacji końcowych w wybranej grupie stacji końcowych z ostatniej godziny. c) Wszystkie aktywności sieciowe dla wszystkich stacji końcowej w wybranej grupie w ostatniej godzinie. d) Wszystkie aktywności w katalogu Temp dla wszystkich stacji końcowych w wybranej grupie z ostatniej godziny. e) Liczbie nieudanych prób logowania per nazwa użytkownika. f) Skryptach Powershell generujących ruch wychodzący per adres IP. g) Skryptach Powershell generujących ruch wychodzący per nazwa stacji końcowej. h) Podejrzanych skryptach Powershell z poleceniami zakodowanymi w base64.
121	Rozwiązanie musi pozwalać na zapisanie przygotowanych zapytań EDR.
122	Rozwiązanie musi pozwalać na uruchomienie poprzednio wykonywanych zapytań EDR
123	Rozwiązanie musi pozwalać wprowadzanie zapytań EDR przy użyciu łatwego i zrozumiałego języka zapytań.
124	Rozwiązanie musi podpowiadać (sugerować) osobie tworzącej zapytanie EDR możliwe opcje.
125	Rozwiązanie musi analizować wprowadzone zapytanie EDR i w czasie rzeczywistym informować czy składnia zapytania jest prawidłowa.
126	Rozwiązanie musi pozwalać na filtrowanie uzyskanych wyników.
127	Rozwiązanie musi automatycznie grupować otrzymane wyniki z uwzględnienie następujących elementów: a) Procesy. b) Komunikacja między procesami. c) Indykatory. d) Pliki. e) Połączenia sieciowe. f) Zapytania DNS. g) Operacje na rejestrze. h) Logi Windows Events. i) Łącza nazwane. j) Operacje logowania. k) Zadania Windows. l) Biblioteki dll.
128	Wszystkie zdarzenia - zbiorcza lista wyświetlająca wszystkie zdarzenia w chronologiczny sposób.
129	Rozwiązanie musi pozwalać na modyfikowanie wprowadzonego zapytania EDR na pomocą wybierania dodatkowych elementów z listy wyników.
130	Rozwiązanie musi pozwalać na wybranie dowolnego elementu z listy wyników zapytania EDR i zaznaczenia go jako incydent bezpieczeństwa.
131	Rozwiązanie musi pozwalać na zapisanie przygotowanych zapytań EDR jako reguł detekcyjnych działających w sposób ciągły, analizujących nowe metadane EDR.

132	Rozwiązanie musi pozwalać na zbieranie metadanych telemetrycznych EDR (z chronionych stacji końcowych) i XDR (z elementów innych niż stacje końcowe).
133	Przechowywanie metadanych telemetrycznych musi trwać co najmniej 14 dni i mieć możliwość rozszerzenia do 5 lat.
134	Funkcjonalność EDR i XDR musi mieć możliwość automatycznego i autonomicznego wykonywania wstępnego indeksowania i wstępnego korelowania zdarzeń, w momencie ich wystąpienia w chronionym środowisku.
135	Indeksowanie powinno odbywać się w czasie rzeczywistym a dostęp do zebranych metadanych telemetrycznych powinien być natychmiastowy.
136	Rozwiązanie musi pozwalać na łatwe przeszukiwanie zgromadzonych metadanych telemetrycznych za pomocą prostego języka zapytań.
137	Rozwiązanie musi pozwalać na wyświetlenie wyników zapytania w czytelny sposób przedstawiając w chronologiczny sposób wszystkie zdarzenia pasujące do zadanego zapytania.
138	Wyniki zapytania powinny być wyświetlone w taki sposób, aby metadane telemetryczne różnych typów były wyświetlane osobno.
139	Rozwiązanie musi pozwalać na wyświetlenie co najmniej następujących typów zdarzeń metadanych telemetrycznych: a) Procesy. b) Komunikacja między procesami. c) Pliki. d) Operacje sieciowe. e) Zapytania DNS-owe. f) URL-e. g) Operacje na rejestrach. h) Operacje na bibliotekach dll. i) Zaplanowane zadania. j) Operacje logowania. k) Operacje wylogowywania. l) Lista komend. m) Łącza nazwane. n) Ładowanie sterowników. o) Windows Even Logs. p) Indykatory. q) Threat Intelligence.
140	Rozwiązanie musi posiadać możliwość automatycznego grupowania powiązanych ze sobą zdarzeń za pomocą unikalnego identyfikatora pozwalającego na łatwą identyfikację wszystkich elementów tej grupy.
141	Wprowadzenie zapytania zawierającego tego typu identyfikator musi zwrócić informację o wszystkich zdarzeniach (IP, DNS, PLIKI, REJESTRY, PROCESY, URL itp.) składających się na daną sytuację, niezależnie od tego czy jest ona związana ze złośliwym oprogramowaniem, czy nie.
142	Rozwiązanie musi pozwalać na ręczne zaznaczenie jakiegokolwiek zdarzenia jako podejrzany lub złośliwy incydent. W wyniku takiego działania rozwiązanie musi automatycznie utworzyć incydent bezpieczeństwa zawierający wszystkie elementy powiązane z zaznaczonym zdarzeniem.
143	Rozwiązanie musi pozwalać na wyświetlenie podsumowania zwróconych danych w taki sposób, aby operator mógł zobaczyć i przeanalizować uzyskane rezultaty, takie jak np. a) Nazwy i liczbę wszystkich procesów zwróconych przez zapytanie. b) Nazwę, ścieżki i liczbę wszystkich plików zwróconych przez zapytanie. c) Źródłowe adresy IP i ich liczbę zwróconą przez zapytanie. d) Docelowe adresy IP i ich liczbę zwróconą przez zapytanie. e) Adresy URL i ich liczbę zwróconą przez zapytanie. f) Nazwy, systemy operacyjne i typy stacji końcowych zwróconych przez zapytanie. g) Typy zapytań i odpowiedzi DNS oraz ich liczbę zwróconą przez zapytanie.
144	Rozwiązanie musi pozwalać na łatwe modyfikowanie wprowadzanych zapytań poprzez dodawanie lub usuwanie dodatkowych argumentów za pomocą wskazywania elementów otrzymanych w poprzednim zapytaniu.

145	Rozwiązanie musi pozwalać na zapisywanie przygotowanych zapytań w celu ich ponownego użycia.
146	Rozwiązanie w przypadku funkcjonalności EDR musi posiadać możliwość szczegółowego definiowania metadanych telemetrycznych które będą zbierane z chronionych stacji końcowych (np. tylko informacje o procesach i zmianach w rejestrze bez kolekcjonowania informacji o operacjach na plikach).
147	Funkcjonalność EDR musi być natywnie zintegrowany z komponentem EPP w jednym autonomicznym agencie.
148	Realizacja funkcjonalności EDR i XDR musi być zgodna z rozporządzeniem RODO (GDPR).
149	Rozwiązanie musi zapewniać przeglądarkę drzewa procesów, w celu uproszczenia i automatyzacji analizy.
150	Rozwiązanie musi pozwalać na tworzenie własnych Dashboardów (pulpitów) wizualizujących wyniki zwróconych zapytań.
151	Stworzone Dashboardy (pulpity) powinny mieć możliwość wyświetlania wyników zwróconych zapytań w określonym czasie, definiowanym przez operatora systemu.
152	Rozwiązanie musi mieć możliwość tworzenia własnych reguł detekcyjnych w oparciu o zbierane metadane telemetryczne.
153	Rozwiązanie musi mieć możliwość stworzenia co najmniej 100 osobnych reguł własnych.
154	Rozwiązanie musi mieć możliwość rozszerzenia liczby własnych reguł do 1000.
155	Rozwiązanie musi wyświetlać ilość zdarzeń, które zostały wygenerowane przez zapisane reguły.
156	Rozwiązanie musi mieć możliwość przypisywania regule jednego z czterech poziomów Severity (niski, średni, wysoki, krytyczny).
157	Rozwiązanie musi mieć możliwość zdefiniowania przedziału czasu do jakiego dana reguła będzie aktywna.
158	Rozwiązanie musi mieć możliwość zdefiniowania reguł działających cały czas bez daty wygaśnięcia.
159	Rozwiązanie musi mieć możliwość tworzenie Incydentu o poziomie Podejrzany lub Złośliwy w momencie wygenerowania zdarzenia. Funkcja ta musi być definiowana podczas budowania reguły.
160	Rozwiązanie musi mieć możliwość dodania stacji końcowej do kwarantanny sieciowej w przypadku zadziałania reguły.
161	Rozwiązanie musi mieć możliwość śledzenia historii zmian poszczególnych reguł.
162	Rozwiązanie musi mieć możliwość łatwego sortowania stworzonych reguł wykorzystując co najmniej następujące elementy: a) Status reguły. b) Rodzaj wygaśnięcia (stała/tymczasowa). c) Czy reguła wygasła. d) Czy reguła osiągnęła limit zdarzeń. e) Czy reguła ma zdefiniowane akcje odpowiedzi. f) Autora reguły. g) Opisu reguły. h) Nazwy reguły.
163	Rozwiązanie musi mieć możliwość przypisania konkretnego skryptu, który będzie wykonywany w momencie zadziałania reguły.
164	Rozwiązanie może posiadać specjalnie przygotowaną wtyczkę do przeglądarki Chrome, która powinna pozwalać na: a) Parsowanie stron WWW w celu wyszukiwania IOC, takich jak: a. MD5. b. SHA1. c. SHA256. d. IP. e. URL. f. Domena.
165	Uruchamianie zapytań Threat Huntingowych w konsoli bazujących na wyszukanych IOC.
166	Przeglądanie i uruchamianie gotowych zapytań Threat Huntingowych przygotowanych przez producenta rozwiązania.

	Rozwiązanie musi posiadać mechanizm kontroli dostępu opartych na rolach (RBAC).
167	Kontrola dostępu oparta na rolach musi być zintegrowana z strukturą konsoli zarządzającej i pozwalać na definiowanie dostępu do całego konta, lub wyłącznie do jednej lub wielu lokalizacji.
168	Rozwiązanie musi umożliwić tworzenie użytkowników serwisowych, którzy nie będą mieli dostępu do interfejsu graficznego konsoli, a dostęp do konsoli będzie realizowany wyłącznie poprzez interfejs API.
169	Rozwiązanie musi oferować predefiniowane role w następujących zakresach zadań: a) Wszystkie funkcje i działania konsoli. b) Tworzy, edytuje i usuwa raporty oraz ma widoczność na cały zakres konsoli. c) Analizuje i reaguje na incydenty z pełną widocznością i tworzy raporty z reakcji na incydenty oraz analizy przyczyn incydentów. d) Zarządza punktami końcowymi, poziomami struktury, wykluczeniami, listami blokowanych i ustawieniami notyfikacji, kontroli urządzeń, kontroli sieci. e) Analizuje i reaguje na zagrożenia z pełnymi uprawnieniami do łagodzenia i usuwania zagrożeń. f) Dostęp tylko do odczytu do funkcji konsoli i danych w przypisanym poziomie struktury rozwiązania.
170	Rozwiązanie musi oferować możliwość tworzenia przez administratorów własnych ról użytkowników z możliwością granularnego definiowania zakresu dostępu do konsoli.
171	Konsola zarządzająca musi wymuszać stosowanie wieloskładnikowego uwierzytelniania dla każdego użytkownika konsoli, niezależnie od roli, która została dla niego przypisana.
172	Dostęp do systemu dla nowego użytkownika musi być realizowany poprzez wiadomość email z konsoli zarządzającej z linkiem weryfikacyjnym, który umożliwi nowemu użytkownikowi zdefiniowanie hasła oraz składnika 2FA.
173	Administrator systemu z odpowiednimi uprawnieniami do zarządzania użytkownikami środowiska musi mieć możliwość do: a) Kasowania użytkowników. b) Tworzenia użytkowników. c) Kopiowanie użytkowników. d) Zmiany roli użytkownika i zakresu dostępu do konsoli. e) Ponowne wysłanie emaila weryfikacyjnego. f) Restartu poświadczeń, w tym 2FA dla wybranego użytkownika lub grupy użytkowników. g) Każdy z użytkowników musi mieć możliwość: h) Tworzenia tokenów API do interakcji z interfejsem API. i) Unieważnienia stworzonego tokenu API. j) Zmiany hasła do systemu.
174	Konsola zarządzająca musi wspierać logowanie SSO (Single Sign-On) z wykorzystaniem protokołu SAML 2.0.
175	Rozwiązanie musi być wyposażone w moduł zarządzania aktywnościami, który będzie prezentował logi związane z konsolą zarządzającą środowiska.
176	Moduł zarządzania aktywnościami musi być zintegrowany z strukturą konsoli zarządzającej i pozwalać na zarządzanie logami w obrębie poszczególnych poziomów struktury.
177	Moduł zarządzania aktywnościami musi oferować możliwość filtrowania logów w następujących kategoriach: a) Zagrożenia. b) Odpowiedź na zagrożenia. c) Zarządzanie incydentami. d) Wykluczenia. e) Operacje administratorskie. f) Detekcja na podstawie reguł. g) Interwał czasowy zdarzeń. h) Email użytkownika konsoli. i) Nazwa hosta.
178	Moduł zarządzania aktywnościami musi oferować możliwość eksportowania wpisów 100, 1000, 5000 lub 10000 ostatnich aktywności do pliku .csv.

179	Moduł zarządzania aktywnościami musi oferować możliwość pobierania logów zebranych przez agenta końcowego po wydaniu komendy z poziomu modułu zarządzania.
180	Rozwiązanie musi mieć możliwość wykonywania inwentaryzacji aplikacji zainstalowanych na stacjach końcowych objętych ochroną.
181	Rozwiązanie musi mieć możliwość prezentowania ilości wersji dla konkretnej aplikacji.
182	Rozwiązanie musi mieć możliwość prezentowania ilości oraz nazw stacji końcowych na których dana aplikacja została zainstalowana.
183	Rozwiązanie musi mieć możliwość filtrowania zebranych informacji z wykorzystaniem co najmniej: a) Nazwy stacji końcowej. b) Nazwy aplikacji. c) Producenta aplikacji. d) Systemu operacyjnego stacji końcowej. e) Wersji systemu operacyjnego. f) Architektury systemu operacyjnego (32/64 bit).
184	Rozwiązanie musi mieć możliwość wykonywania analizy zebranych danych o zainstalowanych aplikacjach pod kontem podatności tych aplikacji.
185	Rozwiązanie musi mieć możliwość wyświetlenia informacji o wykrytych podatnościach dla wykrytych aplikacji podając co najmniej następujące informacje: a) Nazwa aplikacji wraz z jej wersją. b) Producenta aplikacji. c) Poziom Severity dla najwyższej wykrytej podatności. d) Poziom NVD Base Score dla najwyższej wykrytej podatności. e) Liczbę CVE. f) Ilość stacji końcowych. g) Datę wykrycia aplikacji. h) Ilość dni od detekcji.
186	Rozwiązanie musi mieć możliwość filtrowania zebranych informacji na temat podatności z wykorzystaniem co najmniej: a) Nazwy stacji końcowej. b) Nazwy aplikacji. c) Producenta aplikacji. d) Numeru CVE. e) Ilości dni od detekcji.
187	Rozwiązanie musi pozwalać na zarządzanie notyfikacjami i dla każdego typu powiadomień umożliwiać definiowanie zdarzeń jakie mają być notyfikowane.
188	Zarządzanie notyfikacjami musi umożliwiać definiowanie kanału komunikacji (Syslog lub Email) dla każdego rodzaju zdarzenia z osobna. Nie dopuszcza się definicji kanału wyłącznie o typy powiadomień, wymagana jest granularność na poziomie pojedynczego zdarzenia.
189	Zarządzanie notyfikacjami musi umożliwiać wyszukiwanie pojedynczego rodzaju zdarzenia poprzez wyszukiwarkę tekstową.
190	Zarządzanie notyfikacjami musi wyróżniać następujące typy powiadomień: a) Active Directory. b) Administracyjne. c) Własne reguły. d) Kontrola urządzeń. e) Tagi urządzeń. f) Kontrola firewall. g) Lokalizacje. h) Malware. i) Łagodzenie incydentów. j) Operacje. k) Remote Shell. l) Zarządzanie zagrożeniami. m) Wykluczenia / Listy Blokujące.

191	Rozwiązanie musi umożliwiać integrację z serwerem SMTP, aby umożliwić wysyłanie notyfikacji email.
192	Integrację z serwerem SMTP musi umożliwić szyfrowanie notyfikacji poprzez protokół SSL lub TLS.
193	Rozwiązanie musi umożliwiać włączenia notyfikacji email, które będą wysyłane z serwera email dostawcy rozwiązania.
194	Rozwiązanie musi umożliwiać integrację z serwerem Syslog, w celu eksportu logów i notyfikacji z rozwiązania.
195	Rozwiązanie musi umożliwiać wysyłkę logów poprzez Syslog zabezpieczoną protokołem TLS.
196	Rozwiązanie musi umożliwiać przesłanie do konsoli rozwiązania certyfikatów w celu autoryzacji z serwerem Syslog.
197	Komunikacja z serwerem Syslog musi być realizowana za pomocą protokołu UDP, jeżeli nie zostanie ustawiona opcja szyfrowania TLS.
198	Eksport logów po Syslog musi wspierać następujące formaty logów: CEF2, RFC-5424, STIX, IOC.
199	Konsola rozwiązania musi oferować mechanizm testowego połączenia z serwerem Syslog, w celu weryfikacji poprawności konfiguracji.
200	Rozwiązanie musi wspierać protokół SAML 2.0 i integrować się z dostawcami SSO (Single sign-on) zgodnymi z tym protokołem.
201	Rozwiązanie musi wspierać integracje z kontami AWS, która pozwoli weryfikować czy maszyny wirtualne w tej chmurze są chronione za pomocą agentów rozwiązania.
202	Rozwiązanie musi wspierać integracje z tenantami Azure, która pozwoli weryfikować konfigurację i podatności w Azure AD.
203	Rozwiązanie musi umożliwiać integrację z systemami firm trzecich za pomocą aplikacji dostępnych z poziomu konsoli zarządzającej rozwiązania.
204	Aplikacje integrujące rozwiązanie z systemami firm trzecich nie mogą wymagać dodatkowego pisania kodu od administratorów.
205	Aplikacje integrujące muszą być wspierane i zweryfikowane przez producenta rozwiązania.
206	Aplikacje integrujące muszą oferować tryb symulacyjny, który pozwala na zweryfikowanie możliwości i funkcjonalności integracji.
207	Rozwiązanie musi oferować przynajmniej 70 aplikacji integrujących.
208	Rozwiązanie musi oferować następujące kategorie aplikacji integrujących: a) Automatyzacja. b) Backup And Recovery. c) CASB. d) Chat. e) Chmura. f) Logi z platformy chmurowej. g) Aplikacje do współpracy. h) Compliance. i) Ubezpieczenie cyfrowe. j) Bezpieczeństwo poczty elektronicznej. k) Tożsamość. l) Bezpieczeństwo IOT. m) Bezpieczeństwo urządzeń mobilnych. n) Network Detection Response. o) Patching. p) Zarządzanie ryzykiem. q) Sandbox. r) Security Awareness. s) SIEM. t) SOAR. u) Threat Intelligence. v) Threat Response. w) Systemy biletowe.
209	Rozwiązanie musi udostępniać otwarty interfejs API, który będzie umożliwiał obsługę modułów rozwiązania oraz integracje z rozwiązaniami firm trzecich, w przypadku braku aplikacji integrującej.

210	Rozwiązanie musi posiadać pełną dokumentację interfejsu API, która będzie wbudowana w konsolę zarządzającą.
211	Rozwiązanie musi uwierzytelniać zapytania API poprzez token API generowany w konsoli zarządzającej.
212	Rozwiązanie musi umożliwiać wysyłanie zapytań API z poziomu konsoli zarządzającej.
213	Rozwiązanie musi umożliwiać następujące rodzaje grup w ramach tworzonych lokalizacji: a) Grupa statyczna - stacje końcowe są przypisywane manualnie przez administratora do grupy statycznej. Stacje końcowe przenoszą się automatycznie z grup statycznych do grup dynamicznych, jeśli pasują do zdefiniowanego filtra grupy dynamicznej. b) Grupa przypięta - stacje końcowe są przypisywane manualnie przez administratora do grupy przypiętej. Stacje końcowe nie przenoszą się automatycznie z grup przypiętych do grup dynamicznych, nawet jeśli pasują do zdefiniowanego filtra grupy dynamicznej. c) Grupa dynamiczna - stacje końcowe są przypisywane do grupy w oparciu o zdefiniowany filtry. Wszystkie stacje końcowe pasujące do filtra definiującego grupę dynamiczną, są automatycznie przenoszone są do grupy dynamicznej, z wyjątkiem stacjach końcowych w grupach przypiętych.
214	Jeżeli stacja końcowa pasuje do filtra więcej niż jednej grupy dynamicznej, przypisywana jest do grupy o wyższym priorytecie. Priorytet grup dynamicznych musi być definiowany poprzez ranking grup dynamicznych.
215	Migracja stacji końcowej z grupy przypiętej do grupy dynamicznej odbywa się poprzez przeniesienie stacji końcowej do grupy statycznej, skąd stacja końcowa automatycznie zostanie przeniesiona do grupy dynamicznej o najwyższej pozycji w rankingu grup dynamicznej z pasującej do niej filtrem.
216	Dynamiczne grupy muszą umożliwiać wykorzystanie parametrów z Active Directory, bez konieczności bezpośredniej integracji z AD.
217	Rozwiązanie nie może tworzyć struktury grup w oparciu o bezpośrednią integrację z Active Directory, dopuszczone jest wyłącznie wykorzystywanie parametrów pozyskanych przez agentów rozwiązania zainstalowanych na chronionej infrastrukturze.
218	Grupy nie mogą być elementem kontroli dostępu, co oznacza, że użytkownicy konsoli zarządzającej muszą posiadać dostęp na minimalnym poziomie lokalizacji.
219	Rozwiązanie musi umożliwiać oznaczanie hostów poprzez etykiety (tagi).
220	Każda etykieta (tag) musi być określana poprzez dwa parametry - nazwa i wartość etykiety (tagu).
221	Etykiety (tagi) muszą umożliwiać filtrowanie stacji końcowych, tworzenia grup dynamicznych oraz do tworzenie widżetów na pulpicie nawigacyjnym.
222	Etykiety (tagi) muszą być obsługiwane poprzez wydzieloną zakładkę w konsoli zarządzającej, pozwalającej na przeglądanie, tworzenie, edytowanie, sortowanie i wyszukiwanie etykiet.
223	Rozwiązanie musi umożliwiać dopisanie wielu etykiet (tagów) do jednej stacji końcowej.
224	Rozwiązanie musi umożliwiać przypisanie 200 wartości dla każdej nazwy etykiety (tagu).
225	Rozwiązanie musi umożliwiać stworzenie 1000 etykiet (tagów) dla każdego konta i lokalizacji.
226	Wartość etykiety (tagów) musi być elementem opcjonalnym.
227	W momencie migracji stacji końcowej między lokalizacjami w ramach konta: a) Etykieta (tag) przypisana do stacji końcowej jest zachowana, jeśli jest ona zdefiniowana na poziomie struktury, do której stacja końcowa jest migrowana. b) Etykieta (tag) przypisana do stacji końcowej jest usuwana, jeśli nie jest ona zdefiniowana na poziomie struktury, do której stacja końcowa jest migrowana.
228	Rozwiązanie nie może wymagać żadnych uprawnień administracyjnych w usłudze Active Directory ani na kontrolerach domeny.
229	Rozwiązanie nie może instalować żadnych składników oprogramowania na kontrolerach domeny.
230	Rozwiązanie musi obejmować oceny bezpieczeństwa dla Active Directory i Azure Active Directory.
231	Rozwiązanie musi pozwalać na rozszerzenie funkcjonalności ochronnych i wykrywania ataków skierowanych na kontrolery domeny i serwery aplikacyjne zapewniając jednocześnie pojedynczą konsolę do obsługi oceny i wykrywania zagrożeń.
232	Analiza lokalnej usługi Active Directory muszą być wykonywane przez pojedynczy punkt końcowy przyłączony do domeny.
233	Rozwiązanie nie może wymagać łączności VPN między komponentami lokalnymi a konsolą w chmurze.

234	Rozwiązanie musi zapewniać kreatora instalacji ułatwiającego proces wdrożenia.
235	Rozwiązanie musi być w stanie automatycznie wykrywać wiele domen i uwzględniać je w zakresie testów i ochrony.
236	Rozwiązanie musi być w stanie przeprowadzać oceny Azure Active Directory za pośrednictwem interfejsów API dostarczonych przez Microsoft.
237	Rozwiązanie musi przeprowadzać testy w celu wykrycia luk w zabezpieczeniach AD związanych co najmniej z: a) Uwierzytelnianiem. b) Autoryzacją. c) Ustawieniami kont. d) Usługami certyfikatów. e) Uprawnieniami/delegacjami. f) Kwestiami bezpieczeństwa związanymi ze stanem bezpieczeństwa kontrolerów domeny. g) Kwestiami bezpieczeństwa związanymi ze stanem bezpieczeństwa usługi Azure AD.
238	Rozwiązanie musi kategoryzować testy na co najmniej cztery poziomy ważności (severity) od najbardziej krytycznego do niskiego.
239	Rozwiązanie musi być w stanie subskrybować i otrzymywać powiadomienia w czasie rzeczywistym z lokalnej usługi Active Directory (powiadomienia o zmianach).
240	Rozwiązanie musi zawierać pulpit nawigacyjny zapewniający szybki dostęp do informacji o wynikach testów, takich jak: a) Liczba testów per poziom Severity i ich wyniki (zaliczone / niezaliczone / pominięte) łącznie i na testowaną domenę (domeny). b) Wykryta topologia domeny i relacje zaufania między domenami. c) Wynik kondycji i powiązany poziom ryzyka łącznie i indywidualnie dla domeny (domen). d) Najbardziej krytyczne/poważne ustalenia i liczba obiektów, na które mają wpływ. e) Graficzna reprezentacja nieudanych testów w ostatnich uruchomieniach, pozwalająca użytkownikowi szybko zobaczyć wszelkie zmiany w stanie bezpieczeństwa w czasie. f) Rozwiązanie musi zapewniać szerokie możliwości filtrowania wyników testów, w tym co najmniej: g) Poprzednie testy. h) Istotność. i) Nazwa domeny. j) Nazwa lasu. k) Nazwa wykrycia. l) Status potwierdzenia. m) Status podatności. n) Zagrożone komputery. o) Grupa(y), której(ych) dotyczy błąd. p) Użytkownik(cy) objęty(ci) atakiem
241	Rozwiązanie musi umożliwiać porównywanie wyników z poprzednich analiz aż do poziomu poszczególnych testów.
242	Rozwiązanie musi zapewniać następujące szczegóły dotyczące każdego przeprowadzonego testu: a) Opis testu. b) Hiperłącze do odpowiednich stron internetowych MITRE Att&ck. c) Kroki naprawcze. d) Informacje, o narzędziach które mogą wykorzystać wykrytą podatność. e) Hiperłącza do odpowiednich artykułów społeczności bezpieczeństwa Active Directory.
243	Rozwiązanie musi przedstawiać szczegółowe informacje na temat powodów, dla których wykryto luki w zabezpieczeniach, w tym: a) Typy obiektów, np. użytkownik lub grupa. b) Nazwy obiektów. c) Naruszone ustawienia dla każdego obiektu, np. jakie uprawnienia zostały wykryte.
244	Rozwiązanie musi umożliwiać zewnętrzną prezentację wyników testów w postaci raportów PDF i CSV.
245	Raporty muszą uwzględniać wszelkie filtry ustawione przez użytkownika.
246	Raporty muszą określać wszelkie wyjątki wprowadzone przez użytkownika.

247	Obiekty objęte testem muszą być eksportowalne jako CSV na poziomie testu.
248	Rozwiązanie musi być w stanie automatycznie uruchomić pełny cykl testowy zgodnie z harmonogramem konfigurowanym przez użytkownika (np. co X dni), dodać wyniki do bazy danych i wygenerować kompleksowe raporty z testów bez dodatkowej interakcji z użytkownikiem.
249	Rozwiązanie musi obsługiwać doraźne uruchamianie pełnego cyklu testowego i prezentować wyniki w interfejsie GUI oraz w kompleksowych raportach.
250	Rozwiązanie musi obsługiwać uruchamianie poszczególnych testów ad-hoc, bez konieczności uruchamiania pełnego cyklu testowego.
251	Rozwiązanie musi umożliwiać tworzenie i dokumentowanie wyjątków dla przyszłych testów na następujących poziomach: a) Domeny. b) Pojedyncze testy na domenę. c) Pojedyncze obiekty (użytkownik lub grupa) na test i domenę.
252	System musi obsługiwać tworzenie tych wyjątków w centralnej lokalizacji interfejsu GUI lub bezpośrednio z odpowiednich testów/wyników z możliwością dodawania komentarzy dotyczących powodów utworzenia tych wyjątków.
253	Rozwiązanie musi zapewniać szczegółowe wskazówki dotyczące usuwania wykrytych luk w zabezpieczeniach, w tym: a) Linki do taktyk i technik MITRE ATT&CK. b) Kroki przygotowania działań naprawczych. c) Kroki do przeprowadzenia działań naprawczych. d) Linki do dodatkowych informacji z szerszej społeczności bezpieczeństwa Active Directory.
254	Tam, gdzie to możliwe, rozwiązanie musi być w stanie generować skrypty naprawcze, które mogą być wykonywane w odpowiedniej domenie (domenach) z następującymi możliwościami: a) Szczegółowy wybór luk w zabezpieczeniach, które mają zostać naprawione. b) Precyzyjny wybór obiektów, na których będą przeprowadzane działania naprawcze. c) Historia remediacji dotycząca statusu procesu remediacji (wygenerowany skrypt, pobrany, wykonany z wynikiem powodzenia lub niepowodzenia). d) Cofanie skryptów w celu przywrócenia zmian wprowadzonych w ramach wcześniejszych działań naprawczych opartych na skryptach.
255	Rozwiązanie musi być w stanie wykrywać ataki na AD, w tym: a) Niskie i powolne próby siłowe, takie jak "Password Spray". b) Masowe blokady kont. c) Masowe zmiany haseł. d) Masowe wyłączanie/usuwanie kont. e) Podejrzane zmiany haseł dla kont wrażliwych. f) Reaktywacja wyłączonych kont uprzywilejowanych. g) Ataki DCSync. h) Ataki Rouge Domain Controller (DCShadow). i) Używanie domyślnego konta "Administrator". j) Podejrzane tworzenie usług na kontrolerach domeny.
256	Wykrywanie zagrożeń nie może polegać na funkcji zaplanowanej replikacji AD, aby zminimalizować wpływ na Active Directory
257	Musi istnieć możliwość zewnętrznego wykrywania zagrożeń w rozwiązaniach SIEM, SOAR i XDR.
258	Rozszerzając rozwiązanie o funkcje ochrony kontrolerów domeny i serwerów aplikacyjnych, rozwiązanie musi wykrywać co najmniej następujące ataki: a) Golden Ticket. b) Silver Ticket. c) DCSync. d) DCShadow. e) Pass-the-Hash. f) Pass-the-Ticket. g) Odzyskiwanie kont uprzywilejowanych. h) Odzyskiwanie kont usługowych. i) Ataki z użyciem klucza szkieletowego. j) Ataki z użyciem sfałszowanych PAC.

	k) AS REP Roasting.
259	Rozwiązanie musi tłumaczyć język naturalny na ustrukturyzowane zapytania używane przez system i automatycznie wykonywać te zapytania na zbiorze zebranych danych telemetrycznych EDR/XDR.
260	Rozwiązanie musi odpowiadać na pytania dotyczące konfiguracji produktu w języku naturalnym.
261	Rozwiązanie musi umożliwiać tworzenie dodatkowych elementów takich jak np. skryptów Powershell/Bash/Python o które poprosi analityk (np. skrypt w Powershell pokazujący uruchomione usługi na stacji końcowej lub skrypt API w Pythonie pokazujące agentów podłączonych do konsoli).
262	Rozwiązanie musi mieć mechanizm ochrony, który zapobiega niewłaściwemu wykorzystaniu systemu przez użytkowników i jest odporny na ataki na LLM.
263	Rozwiązanie musi mieć koncepcję konwersacji, która powinna pozwolić zadawać pytania i otrzymywać odpowiedzi w określonym kontekście (np. zakres czasowy ostatnich trzech dni).
264	Rozwiązanie musi podsumowywać analizowane zdarzenia i wskaźniki przy użyciu języka naturalnego.
265	Rozwiązanie musi rekomendować kolejne pytania, które można zadać w trakcie procesu prowadzonego śledztwa.
266	Rozwiązanie musi mieć możliwość tworzenia podsumowujących wiadomości e-mail po zakończeniu procesu prowadzonego śledztwa.
267	Rozwiązanie musi mieć możliwość zbierania opinii użytkowników na temat wyników "tłumaczenia języka naturalnego na ustrukturyzowane zapytania" i zwróconych wyników.
268	Rozwiązanie musi pozwalać na udostępnienie wyników śledztwa innym członkom zespołu.
269	Rozwiązanie musi mieć "niski próg wejścia" poprzez implementację przykładowych zapytań, które mogą być zadawane przez analityków bezpieczeństwa.
270	Rozwiązanie nie może być szkolone przy użyciu telemetrii klienta, zapytań i wyników zapytań.
271	Rozwiązanie musi przedstawiać podsumowanie konkretnego incydentu bezpieczeństwa w języku naturalnym opisując co zostało wykryte i co się wydarzyło.