Numer sprawy: **Izp.271.33.2024 Załącznik numer 6b do SWZ**

**Zadanie nr 2**

Spis treści

[1 ZASILACZ AWARYJNY UPS - 2 KPL. 3](#_Toc178600331)

[2 BIBLIOTEKA TAŚMOWA WRAZ Z NOŚNIKAMI TAŚMOWYMI - 1 kpl 7](#_Toc178600332)

[3 ZARZĄDZALNE PRZEŁĄCZNIKI – 2 szt 13](#_Toc178600333)

[4 SERWER NAS WRAZ OPROGRAMOWANIEM I Z DYSKAMI TYP I - 1 KPL 18](#_Toc178600334)

[5 SERWER NAS WRAZ OPROGRAMOWANIEM I Z DYSKAMI TYP II - 1 KPL 22](#_Toc178600335)

[6 KOMPATYBILNE DYSKI HDD DO POSIADANEGO SERWERA SYNOLOGY RS1221RP+ - 4 SZT. 25](#_Toc178600336)

[7. SERWER WIRTUALIZACYJNY Z SYSTEMEM OPERACYJNYM I OPROGRAMOWANIEM BAZODANOWYM – 1 kpl 26](#_Toc178600337)

[8 SYSTEM NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO – 220 IP 46](#_Toc178600338)

[9. SYSTEM DETEKCJI I REAKCJI NA ZDARZENIA W KOŃCOWYCH PUNKACH – EDR – 120 licencji 55](#_Toc178600339)

[10. SYSTEM ZARZĄDZANIA INFORMACJAMI I ZDARZENIAMI BEZPIECZEŃSTWA INFORMATYCZNEGO - SIEM 81](#_Toc178600340)

[11. SYSTEM ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP) - 150 LICENCJI 90](#_Toc178600341)

[12. OPROGRAMOWANIE ANTYWIRUSOWE DEDYKOWANE DO SERWERÓW- 15 licencji 108](#_Toc178600342)

[13 WDROŻENIE I SZKOLENIE 131](#_Toc178600343)

[A WDROŻENIE SERWERA WIRTUALIZACYJNEGO Z SYTEMEM BAZODANOWYM i BIBLIOTEKI TAŚMOWEJ 131](#_Toc178600344)

[B WDROŻENIE I SZKOLENIE SERWERA NAS 135](#_Toc178600345)

[C WDROŻENIE I SZKOLENIE PRZEŁĄCZNIKÓW 143](#_Toc178600346)

[D Wdrożenie i SZKOLENIE SYSTEMU NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO 145](#_Toc178600347)

[E Wdrożenie i SZKOLENIE SYSTEMU ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP) 146](#_Toc178600348)

[F WDROŻENIE I SZKOLENIE SYSTEMÓW SYSTEM DETEKCJI I REAKCJI NA ZDARZENIA W KOŃCOWYCH PUNKACH – EDR 148](#_Toc178600349)

[SYSTEMU ZARZĄDZANIA INFORMACJAMI I ZDARZENIAMI BEZPIECZEŃSTWA INFORMATYCZNEGO - SIEM 148](#_Toc178600350)

[OPROGRAMOWANIA ANTYWIRUSOWEGO DEDYKOWANE DO SERWERÓW 148](#_Toc178600351)

## 1 ZASILACZ AWARYJNY UPS - 2 KPL.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Dane producenta | Podać dane producenta i model seria | **Producent:    Model wersja:** |
|  | Moc pozorna | min. 6000VA | SPEŁNIA TAK /NIE |
|  | Moc rzeczywista | min. 6000W | SPEŁNIA TAK /NIE |
|  | Technologia | on-line (VFI), podwójna konwersja | SPEŁNIA TAK /NIE |
|  | Sprawność przy pracy sieciowej | ˃ 95 % | SPEŁNIA TAK /NIE |
|  | Sprawność przy pracy bateryjnej | ˃ 92 % | SPEŁNIA TAK /NIE |
|  | Typ obudowy | rack/tower | SPEŁNIA TAK /NIE |
| **Wejście** | | | |
|  | Napięcie wejściowe | 208/220/230/240 VAC | SPEŁNIA TAK /NIE |
|  | Częstotliwość napięcia wejściowego | 46~54 Hz lub 56~64 Hz | SPEŁNIA TAK /NIE |
|  | Zakres napięcia wejściowego | 110 ÷ 300 V AC ± 3% przy 50% obciążenia | SPEŁNIA TAK /NIE |
|  | Kształt napięcia wyjściowego | sinusoidalny | SPEŁNIA TAK /NIE |
|  | Czas przełączania sieć – bateria | 0ms | SPEŁNIA TAK /NIE |
|  | Współczynnik odkształceń prądu wejściowego THDi | 3% przy 100% obciążenia | SPEŁNIA TAK /NIE |
| **Wyjście** | | | |
|  | Napięcie wyjściowe | 208/220/230/240 VAC | SPEŁNIA TAK /NIE |
|  | Częstotliwość napięcia wyjściowego | 50Hz/60Hz ± 0,1Hz | SPEŁNIA TAK /NIE |
|  | Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny | SPEŁNIA TAK /NIE |
|  | Współczynnik odkształceń prądu wejściowego THD | ≦ 2 % (obciążenie liniowe); ≦ 6 % (obciążenie nieliniowe) | SPEŁNIA TAK /NIE |
|  | Baterie wewnętrzne w UPS lub w zewnętrznym module bateryjnym | minimum 12V 9Ah; szczelne, bezobsługowe | SPEŁNIA TAK /NIE |
|  | Czas podtrzymania (100 % Pmax) - przy zastosowaniu wewnętrznych baterii lub w zewnętrznym module bateryjnym | minimum 9 minut | SPEŁNIA TAK /NIE |
| **Pozostałe** | | | |
|  | Prąd ładowania baterii | minimum 4A | SPEŁNIA TAK /NIE |
|  | Współpraca z 16 lub 20 bateriami | wymagane | SPEŁNIA TAK /NIE |
|  | Wejście zasilania | listwa zaciskowa / terminal śrubowy | SPEŁNIA TAK /NIE |
|  | Ilość i typ gniazd wyjściowych | listwa zaciskowa / terminal śrubowy | SPEŁNIA TAK /NIE |
|  | obciążalność w trybie sieciowym AC | 100%~110%:10min; 110%~130%:1min; >130%:1s | SPEŁNIA TAK /NIE |
|  | Sygnalizacja | Wyświetlacz LCD, diody LED | SPEŁNIA TAK /NIE |
|  | Informacje wyświetlane na panelu LCD | minimum poziom obciążenia (w %),  poziom naładowania baterii (w %),  praca z sieci/baterii/ładowanie baterii,  przeciążenie, niski poziom baterii,  bateria nie podłączona lub błąd baterii, tryb ECO/Bypass,  napięcie wej/wyj,  czętotliwość wej/wy błąd + numer błędu, czas podtrzymania bateryjnego,  wyłączenie dźwięku, | SPEŁNIA TAK /NIE |
|  | Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych (producenta) | wymagane | SPEŁNIA TAK /NIE |
|  | Interfejs komunikacyjny | RS232, USB, SNMP | SPEŁNIA TAK /NIE |
|  | Gniazdo na kartę rozszerzeń - np.. SNMP | wymagane | SPEŁNIA TAK /NIE |
|  | Wsporniki do montażu w szafie RACK | wymagane | SPEŁNIA TAK /NIE |
|  | Zewnętrzny Bypass bezprzerwowy w wersji RACK | wymagane | SPEŁNIA TAK /NIE |
|  | Zewnętrzny czujnik temperatury i wilgotności SNMP | wymagane | SPEŁNIA TAK /NIE |
|  | Zabezpieczenia | minimum przeciwzwarciowe, przeciwprzepięciowe, przeciążeniowe | SPEŁNIA TAK /NIE |
|  | Złącze EPO | wymagane | SPEŁNIA TAK /NIE |
|  | Waga UPS | do 18 kg | SPEŁNIA TAK /NIE |
|  | Wymiary UPS - wersja RACK | nie większe niż: wysokość 2U; głębokość 620 mm | SPEŁNIA TAK /NIE |
|  | Waga Moduł Bateryjny - jeżeli występuje | do 49 kg | SPEŁNIA TAK /NIE |
|  | Wymiary Moduł Bateryjny - wersja RACK - jeżeli występuje | nie większe niż: wysokość 3U; głębokość 720 mm | SPEŁNIA TAK /NIE |
|  | Gwarancja | minimum 12 miesięcy na elektronikę i 12 miesięcy na akumulatory; | SPEŁNIA TAK /NIE |
|  | Serwis | autoryzowany serwis producenta zlokalizowany w Polsce. | SPEŁNIA TAK /NIE |
| naprawa w maksymalnie 48 godzin roboczych, w przypadku przekroczenia terminu Wykonawca dostarczy urządzenie zastępcze . Na poświadczenie tego faktu, Wykonawca załączy do oferty Oświadczenie Producenta/lub autoryzowanego Dystrybutora iż naprawa będzie wykonana we współpracy z Autoryzowanym Partnerem Serwisowym Producenta oferowanego sprzętu o spełnieniu tego wymogu. | SPEŁNIA TAK /NIE |
| gwarancja realizowana wyłącznie przez Autoryzowany Serwis Producenta | SPEŁNIA TAK /NIE |
|  | Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS | SPEŁNIA TAK /NIE |
| wsparcie dla systemów: Windows, Windows Server, Linux oraz systemów wirtualizacji: VMware i Hyper-V. | SPEŁNIA TAK /NIE |
| wymagane techniczne wsparcie producenta (telefoniczne oraz mailowe) w języku polskim. | SPEŁNIA TAK /NIE |
| Oferent dostarczy jedno wspólne oprogramowanie do zarzadzania i monitorowania wszystkich proponowanych zasilaczy UPS. Oprogramowanie powinno być wskazane przez producenta zasilaczy UPS. Nie dopuszcza się możliwości dostosowywania oprogramowania innych producentów np. za pomocą skryptów. | SPEŁNIA TAK /NIE |
|  | Możliwość monitorowania i konfiguracji UPS przez przeglądarkę WWW | wymagane | SPEŁNIA TAK /NIE |
|  | **Certyfikaty producenta (załączyć do oferty)** | 1. **Oświadczenie Producenta lub autoryzowanego dystrybutora o naprawie oferowanego UPS maksymalnie do 48 godzin roboczych, w przypadku przekroczenia terminu Wykonawca dostarczy urządzenie zastępcze** 2. **deklaracja zgodności CE** | SPEŁNIA TAK /NIE |
|  | **karta produktowa oferowanego sprzętu** | SPEŁNIA TAK /NIE |
|  | **Instalacja** | Podłączenie do przygotowanej instalacji elektrycznej przez Autoryzowany Serwis Producenta uwzględniające podłączenie UPS, podłączenie modułu bateryjnego (jeżeli występuje), podłączenie bypassu do wejścia zasilania oraz do UPSa, montaż . Szkolenie minimum 3 godziny w siedzibie Zamawiającego. | SPEŁNIA TAK /NIE |

## 2 BIBLIOTEKA TAŚMOWA WRAZ Z NOŚNIKAMI TAŚMOWYMI - 1 kpl

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Ogólne | Biblioteka, do sporządzania archiwum i składowania danych na taśmach , dla zwiększenie bezpieczeństwa danych, | Producent  Model wersja |
|  | Komponent | Minimalne wymagania | SPEŁNIA TAK /NIE |
|  | Obudowa i pojemność | Wysokosć maksymalnie 1U do instalacji w szafie Rack.  Co najmniej 9 slotów przeznaczonych na zestaw taśm. | SPEŁNIA TAK /NIE |
|  | Połączenie | Co najmniej 1 port SAS o przepustowości co najmniej 12Gb/s w standardzie umożliwiającym podłączenie serwerów. | SPEŁNIA TAK /NIE |
|  | Napęd | Wyposażony w co najmniej 1 sztukę napędu SAS LTO9.  W komplecie:   * 5x taśma LTO9 * Etykiety do taśm o numerach 1-200 * 1x taśma czyszcząca | SPEŁNIA TAK /NIE |
|  | Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego,  automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.  Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.  Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.  Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.  Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury.  Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :   * Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. * Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. * Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :   a. o poprawkach i usprawnieniach dotyczących aktualizacji  b. dacie wydania ostatniej aktualizacji  c. priorytecie aktualizacji  d. zgodność z systemami operacyjnymi  e. jakiego komponentu sprzętu dotyczy aktualizacja  f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.   * wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne * możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. * - rozpoznanie modelu oferowanego urządzenia numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr ) * sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania ) * dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml * raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. | Producent  nazwa i wersja oprogramowania  SPEŁNIA TAK /NIE |
|  | Gwarancja | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lata. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokument potwierdzony przez Producenta/lub autoryzowanego Dystrybutora, należy załączyć do oferty. * Wymagane dołączenie do oferty oświadczenia Producenta/lub autoryzowanego Dystrybutora, potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. | SPEŁNIA TAK /NIE |
|  | Oprogramowanie do backupu danych na taśmach | * **Możliwośc backupu licencja na 25 serwerów, 5 hostów wirtualizacji** * Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich * Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology * Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology * Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) * **Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)** * Automatyczny **backup przy wyłączaniu komputera** * Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ? * Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) * Backup baz danych i plików poczty w trybie online i offline * Kopie rotacyjne (wersjonowanie) * **Zapis archiwów w otwartym formacie (ZIP 64-bit)** * Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi * Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) * Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej * Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych * Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO * Kompresja po stronie stacji roboczej * Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, * Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) * Centralne sterowanie całym Systemem z jednego miejsca * Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników * Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN * Wysyłanie Alertów administracyjnych na e-mail * Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych * Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki * Automatyczna aktualizacja oprogramowania na komputerach zdalnych * Bezterminowa licencja - licencja nie może być ograniczona czasowo * Interfejs, instrukcja i pomoc techniczna w języku polskim | Producent oprogramowania  Nazwa i wersja  SPEŁNIA TAK /NIE |

## 3 ZARZĄDZALNE PRZEŁĄCZNIKI – 2 szt

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne) Oferowane parametry** |  |
|  | Charakterystyka ogólna | Przełącznik zarządzalny do szafy rack , zwiększający posiadane zasoby , do wzmocnienia segmentacji sieci , i zwiększenia bezpieczeństwa :  48 x 1000Base-T IEEE 802.3ab  Obsługa IEEE 802.3x Flow Control (Full-Duplex) oraz Back Pressure (Half-Duplex), Auto MDI/MDI-X na wszystkich portach  Możliwość konfiguracji prędkości i dupleksu oraz wyłączenia FlowControl dla każdego portu  4 x SFP+ IEEE 802.3ae/802.3ae - porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z  Konsola szeregowa RS-232  Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie | **Producent:**    **Model wersja**  SPEŁNIA TAK /NIE |
| Zasilanie AC 230V  Pojemność przełączania nie mniej, niż 176 Gb/s. Wydajność przełączania nie mniej niż 130 Mp/s.  Architektura nieblokującą (wire-speed).  Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych  Ilość RAM nie mniej, niż 256 MB. Pamięć Flash nie mniej, niż 32 MB  Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B  Bufor pakietów nie mniej, niż 3 MB  Temperatura pracy w zakresie co najmniej od -5ºC do 50ºC.  MTBF > 410000 godzin. |  |
|  | Funkcjonalności warstwy 2 | IGMP Snooping v3 - obsługa nie mniej, niż 500 grup multicast, w tym co najmniej 256 grup statycznych  MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast, w tym co najmniej 31 grup statycznych  IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN  Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP  Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie. Obsługa LACP  LLDP (802.1AB) oraz LLDP-MED.  ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni  DHCP Relay (opcje 60 i 61), opcja 82, DHCP Local Relay (opcja 82). DHCP Relay dla IPv6  Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu | SPEŁNIA TAK /NIE |
| Obsługa sieci VLAN  802.1Q VLAN (nie mniej, niż 4094), 802.1v, GVRP  Surveillance VLAN  MAC-based VLAN  Asymmetric VLAN  Funkcjonalności warstwy 3  Wiele interfejsów IPv4 (co najmniej 16 instancji)  UDP helper  DHCP Server (co najmniej 10 pul adresowych), DHCPv6 Server (co najmniej 16 pul adresowych)  Tablica ARP co najmiej 0,5K (co najmniej 256 wpisów statycznych)  Pojemność tablicy przekazywania co najmniej 512 tras IPv4 oraz 256 takich tras dla IPv6  Pojemność tablicy routowania co najmniej 64 tras IPv4 oraz 32 takich tras dla IPv6.  Routing statyczny IPv4 (co najmniej 64 tras) oraz IPv6 (co najmniej 32 tras)  IPv6 ND  Quality of Service  QoS - co najmniej 8 kolejek. Klasyfikacja w oparciu o: port fizyczny, VLAN, MAC, EtherType, IP, DSCP, protokół, port TCP/UDP, klasa IPv6, etykieta IPv6  Mapowanie DSCP do COS  Obsługa algorytmu Strict, WRR, WDRR  Obsługa trTCM/srTCM  Limitowanie pasma TX per port (nie więcej niż co 64 kb/s)  Limitowanie pasma RX per port (nie więcej niż co 64 kb/s)  Filtrowanie ruchu |  |
| ACL w oparciu o: port przełącznika, MAC, VLAN, 802.1p, IP, DSCP, typ protokołu, port TCP/UDP, klasę IPv6, etykietę IPv6, uruchamianie reguł ACL wg kalendarza, definiowanie reguł VLAN ACL | SPEŁNIA TAK /NIE |
|  | Funkcje bezpieczeństwa | Port Security (co najmniej 120 adresów MAC per port). Funkcja Port Security Shutdown  Uwierzytelnianie 802.1X z obsługą Guest VLAN  Możliwość jednoczesnego uwierzytelniania wielu użytkowników 802.1X na porcie  Przypisywanie parametrów autoryzacyjnych z serwera RADIUS: VLAN, 802.1p, przepustowość portu, reguły ACL  Obsługa CoA  Uwierzytelnianie poprzez stronę Web  Uwierzytelnianie po MAC  Uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.  Filtrowanie w oparciu o pary IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), DHCP Snooping, Dynamic ARP Inspection (również IPv6)  Separacja klientów przyłączonych do różnych portów  Blokowanie serwerów DHCP  MAC Blackholing  ARP Spoofing Prevention  BPDU Attack Protection  DoS Attack Protection  Unicast Storm Control (krok co najwyżej 64Kbps i 2pps), Multicast Storm Control (krok co najwyżej 64Kbps i 2pps), Broadcast Storm Control (krok co najwyżej 64Kbps i 2pps), Storm Control Port Shutdown, Storm Control Port Recovery |  |
|  | Zarządzanie | Uwierzytelnianie dostępu administracyjnego protokołem RADIUS i TACACS+.  Zarządzanie stosem poprzez pojedynczy adres IP  Zdalne wykrywanie urządzenia przez dedykowaną aplikację producenta przełącznika i co najmniej zmiana adresu IP urządzenia  WebGUI (obsługa IPv6), Telnet (co najmniej 4 sesji jednoczesnych) (obsługa IPv6), SSH (obsługa IPv6), konsola szeregowa (możliwość wprowadzania poleceń, możliwość konfiguracji wszystkich funkcjonalności urządzenia)  Wsparcie szyfrowania HTTP  Możliwość wykrywania urządzeń zgodnych z protokołem ONVIF, wyświetlanie informacji o rzeczywistym stanie tych urządzeń  SNMPv2, v3 (obsługa IPv6)  RMON, sFlow  Obsługa DDM  Klient DHCP oraz provisioning z zewnętrznego serwera TFTP  Klient DNS  Klient SNTP (obsługa IPv6)  Zapis logów na serwer Syslog (obsługa IPv6)  Zapis i pobieranie konfiguracji z serwera TFTP  Traceroute  Diagnostyka okablowania (co najmniej pomiar długości oraz ciągłość połączenia).  Możliwość wprowadzania opisów portów.  Wysyłanie powiadomień SNMP po pojawieniu się nowego adresu MAC w sieci.  Możliwość logowania wydawanych poleceń.  Możliwość przechowywania wielu wersji firmware.  Wsparcie 802.3az (Energy Efficient Ethernet). |  |
| Zmniejszanie pobieranej mocy poprzez wykrywanie aktywności linku na portach, administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych. |  |
|  | Pozostałe | Dostępność bezpłatnych aktualizacji oprogramowania przez cały czas życia produktu.  Gwarancja minimum 36 m-cy. | SPEŁNIA TAK /NIE |
|  | **Dodatkowe akcesoria** | Szyny do instalacji w szafie teleinformatycznej Zamawiającego , kable do stackowania minimum 2 szt 1 m | SPEŁNIA TAK /NIE |

## 4 SERWER NAS WRAZ OPROGRAMOWANIEM I Z DYSKAMI TYP I - 1 KPL

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Cechy ogólne | Serwer NAS z przeznaczeniem do wdrożenia rozwiązania wersjonowania plików celem zwiększenia bezpieczeństwa i integralności danych, w przypadku zagrożeń cybernetycznych | **Producent:**  **Model wersja:** |
|  | Obudowa | Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie. Obudowa musi zawierać minimum 2 kontrolery pracujące w układzie nadmiarowym typu active‐passive. | SPEŁNIA TAK /NIE |
|  | Procesor | Jeden procesor osiągający wynik minimum 5400 punktów w teście PassMark na każdy kontroler. | SPEŁNIA TAK /NIE |
|  | Pamięć RAM | Minimum 32GB DDR4 ECC w konfiguracji 2 x 16GB na każdy kontroler. Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników. | Producent  Model pamięci  SPEŁNIA TAK /NIE |
|  | Ilość obsługiwanych dysków | Minimum **12 dysków** o maksymalnej pojemności nie mniejszej niż 16TB każdy, po podłączeniu modułów rozszerzających minimum **36 dysków**.. | SPEŁNIA TAK /NIE |
|  | Zainstalowane dyski | 7 dysków o pojemności 12TB każdy zgodnych z listą kompatybilności oferowanego rozwiązania oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM,  - pamięć cache: minimum 250 MB,  - gwarancja: minimum 36 miesięcy,  - MTBF: minimum 2,5 miliona.  W przypadku awarii dysku twardego uszkodzony nośnik pozostaje własnością Zamawiającego. | Producent  Model wersja  SPEŁNIA TAK /NIE |
|  | Interfejsy sieciowe | Minimum 2 porty 1GbE RJ-45 na kontroler.  Minimum 1 port 10GbE RJ-45 na kontroler.  Wsparcie dla Link Agregation. Możliwość rozszerzenia o dodatkowe 2 porty 10Gb SFP+ / RJ-45. | SPEŁNIA TAK /NIE |
|  | Wskaźniki LED | Status, HDD 1-12, zasilanie, LAN 1-3 | SPEŁNIA TAK /NIE |
|  | Obsługa RAID | RAID 0, 1, 5, 6, 10 wraz z obsługą dysków typu hot spare. | SPEŁNIA TAK /NIE |
|  | Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | SPEŁNIA TAK /NIE |
|  | Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | SPEŁNIA TAK /NIE |
|  | Protokoły | SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | SPEŁNIA TAK /NIE |
|  | Usługi | 1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antywirus, Klient VPN, Usługa DDNS, Zarządzanie przez Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V 2016 i 2019 (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo:  • Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK.  • Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0.  • W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych.  • Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu.  • Kopia zapasowa bez agentów.  • Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej  • Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych.  • Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS.  • W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, I ext4.  • Kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS).  • Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V.  3. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu. | SPEŁNIA TAK /NIE |
|  | Obsługa migawek | Liczba migawek folderu współdzielonego: minimum 1000 | SPEŁNIA TAK /NIE |
|  | Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. | SPEŁNIA TAK /NIE |
|  | Język GUI | Polski | SPEŁNIA TAK /NIE |
|  | Gwarancja i serwis | Minimum 36 m-cy gwarancji Next Business Day producenta – dostawa sprzętu zastępczego w przypadku awarii na następny dzień roboczy. | SPEŁNIA TAK /NIE |
|  | Waga bez dysków | Maksymalnie 25 kg | SPEŁNIA TAK /NIE |
|  | Pobór mocy | Maksymalnie 450W w trybie pracy. | SPEŁNIA TAK /NIE |
|  | Certyfikaty | CE, FCC | SPEŁNIA TAK /NIE |
|  | System plików | Dyski wewnętrzne: BTRFS. | SPEŁNIA TAK /NIE |
|  | Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) | SPEŁNIA TAK /NIE |
|  | Liczba wolumenów | Minimum 60 | SPEŁNIA TAK /NIE |
|  | Liczba iSCSI Targetów | Minimum 250 | SPEŁNIA TAK /NIE |
|  | Liczba iSCSI LUN | Minimum 250 | SPEŁNIA TAK /NIE |
|  | Liczba kont lokalnych użytkowników | Minimum 10000 | SPEŁNIA TAK /NIE |
|  | Liczba grup | Minimum 500 | SPEŁNIA TAK /NIE |
|  | Liczba folderów udostępnionych | Minimum 500 | SPEŁNIA TAK /NIE |
|  | Ilość jednoczesnych połączeń dla CIFS/AFP/FTP | Minimum 1200 | SPEŁNIA TAK /NIE |
|  | Zasilacz | Redundantny zasilacz o mocy minimalnej 500W. | SPEŁNIA TAK /NIE |
|  | Chłodzenie | Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy. | SPEŁNIA TAK /NIE |

## 5 SERWER NAS WRAZ OPROGRAMOWANIEM I Z DYSKAMI TYP II - 1 KPL

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  |  | Serwer NAS z przeznaczeniem do wdrożenia rozwiązania kopii odmiejscowionej , oraz składowania logów z oprogramowania do agregacji i kategoryzacji logów z całej infrastruktury | **Producent:**  **Model wersja:** |
|  | Procesor | Wielordzeniowy procesor osiągający wynik minimum 4 tys. punktów w teście PassMark. | SPEŁNIA TAK /NIE |
|  | Obudowa | Typu rack o wysokości maksymalnej 2U z szynami przesuwnymi do instalacji w szafie rack w zestawie. | SPEŁNIA TAK /NIE |
|  | Pamięć RAM | Minimum 4GB DDR4 ECC (1 x 4GB). | SPEŁNIA TAK /NIE |
|  | Interfejsy sieciowe | Minimum 4 porty 1GbE RJ-45.  Obsługa agregacji łączy. | SPEŁNIA TAK /NIE |
|  | Ilość obsługiwanych dysków | Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków. | SPEŁNIA TAK /NIE |
|  | Zainstalowane dyski | 6 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego rozwiązania oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 60 miesięcy, - MTBF: minimum 2 miliony.  Możliwość aktualizacji oprogramowania dysków bezpośrednio z interfejsu systemu operacyjnego serwera NAS. | PRODUCENT  NAZWA I MODEL  SPEŁNIA TAK /NIE |
|  | Gniazda rozszerzeń | 1 slot PCIe 3.0 x8 | SPEŁNIA TAK /NIE |
|  | Wskaźniki LED | Status, HDD 1-8, zasilanie, LAN 1-4 | SPEŁNIA TAK /NIE |
|  | Obsługa RAID | Pojedynczy, JBOD, RAID 0, 1, 5, 6, 10, SHR wraz z obsługa dysków typu hot spare. | SPEŁNIA TAK /NIE |
|  | Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | SPEŁNIA TAK /NIE |
|  | Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | SPEŁNIA TAK /NIE |
|  | Protokoły | SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP | SPEŁNIA TAK /NIE |
|  | Usługi | 1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. | SPEŁNIA TAK /NIE |
|  | Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, | SPEŁNIA TAK /NIE |
|  | Język GUI | Polski | SPEŁNIA TAK /NIE |
|  | Gwarancja i serwis | Minimum 60 miesięcy gwarancji producenta działającej w trybie 5/13 NBD na cały system złożony z serwera, dysków i akcesoriówz opcją pozostawienia uszkodzonego nośnika u Zgłaszającego. Dostawa sprzętu zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej. | SPEŁNIA TAK /NIE |
|  | Waga bez dysków | Maksymalnie 10 kg | SPEŁNIA TAK /NIE |
|  | Typowy pobór mocy podczas pracy | Maksymalnie 70W | SPEŁNIA TAK /NIE |
|  | Certyfikaty | CE, FCC | SPEŁNIA TAK /NIE |
|  | System plików | Dyski wewnętrzne: BTRFS | SPEŁNIA TAK /NIE |
|  | Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) | SPEŁNIA TAK /NIE |
|  | Liczba wolumenów | Minimum 64 | SPEŁNIA TAK /NIE |
|  | Liczba iSCSI Targetów | Minimum 125 | SPEŁNIA TAK /NIE |
|  | Liczba iSCSI LUN | Minimum 250 | SPEŁNIA TAK /NIE |
|  | Liczba kont użytkowników | Minimum 2000 | SPEŁNIA TAK /NIE |
|  | Liczba grup | Minimum 255 | SPEŁNIA TAK /NIE |
|  | Liczba folderów udostępnionych | Minimum 500 | SPEŁNIA TAK /NIE |
|  | Ilość jednoczesnych połączeń | Minimum 1000 | SPEŁNIA TAK /NIE |
|  | Zasilanie | Redundantny zasilacz o mocy minimum 300W | SPEŁNIA TAK /NIE |

## 6 KOMPATYBILNE DYSKI HDD DO POSIADANEGO SERWERA SYNOLOGY RS1221RP+ - 4 SZT.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Dane producenta /model | Producent oferowanego rozwiązania /model i wersja modelu | **Producent:**  **Model wersja:** |
|  | Rozmiar dysku | 3.5” | SPEŁNIA TAK /NIE |
|  | Interfejs | SATA 6Gb/s | SPEŁNIA TAK /NIE |
|  | Pojemność | Minimum 8TB | SPEŁNIA TAK /NIE |
|  | Prędkość obrotowa | 7200 RPM | SPEŁNIA TAK /NIE |
|  | MTBF | Minimum 2 miliony | SPEŁNIA TAK /NIE |
|  | Gwarancja | Minimum 36 miesięcy | SPEŁNIA TAK /NIE |

## 7. SERWER WIRTUALIZACYJNY Z SYSTEMEM OPERACYJNYM I OPROGRAMOWANIEM BAZODANOWYM – 1 kpl

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Charakterystyka ogólna | Serwer będzie przeznaczony do instalacji oprogramowania zwiększającego poziom cyberbezpieczeństwa w środowisku Zamawiającego. Na serwerze będą instalowane i dostępne narzędzia do ochrony sieci, takie jak system NAC , systemy DLP do ochrony przed wyciekiem danych , narzędzie do monitorowania i analizy ruchu sieciowego, oprogramowanie do kategoryzacji i składowanai LOG . Jego przeznaczenie to ochrona infrastruktury IT przed zagrożeniami, zarządzaniem dostępem do zasobów oraz zapewnieniem bezpieczeństwa | **Producent:**  **Model wersja:** |
|  | Obudowa | * Obudowa Rack o wysokości max 2U z możliwością instalacji 12 dysków 3.5” * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. | SPEŁNIA TAK /NIE |
|  | Płyta główna | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. | SPEŁNIA TAK /NIE |
|  | Chipset | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | SPEŁNIA TAK /NIE |
|  | Procesor | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. | SPEŁNIA TAK /NIE |
|  | RAM | * Nie mniej niż 256GB DDR5 RDIMM 5600MT/s, | SPEŁNIA TAK /NIE |
|  | Funkcjonalność pamięci RAM | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) | SPEŁNIA TAK /NIE |
|  | Kontroler RAID | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących | SPEŁNIA TAK /NIE |
|  | Dyski twarde | * Zainstalowane:   + 2x dysk SSD SATA o pojemności min. 1.92TB, Hot-Plug   + 8x dysk HDD SATA o pojemności min. 8TB 6Gbps Hot-Plug * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. | SPEŁNIA TAK /NIE |
|  | Gniazda PCI | * Cztery sloty PCIe | SPEŁNIA TAK /NIE |
|  | Interfejsy sieciowe/FC/SAS | * Wbudowane 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Czteroportowa karta sieciowa 1Gb Ethernet BaseT * Dwuportowa karta sieciowa 10Gb Ethernet BaseT * Czteroportowa karta 12Gb SAS HBA | SPEŁNIA TAK /NIE |
|  | Wbudowane porty | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudwy * Możliwość rozbudowy o port RS232 | SPEŁNIA TAK /NIE |
|  | Video | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 | SPEŁNIA TAK /NIE |
|  | Wentylatory | * Redundantne, Hot-Plug | SPEŁNIA TAK /NIE |
|  | Zasilacze | * Redundantne, Hot-Plug min. 1100W klasy Titanium | SPEŁNIA TAK /NIE |
|  | Elementy montażowe | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych | SPEŁNIA TAK /NIE |
|  | System operacyjny/dodatkowe oprogramowanie | * Windows Server 2022 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych. * Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania: * Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. * Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. * Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. * Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. * Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. * Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. * Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. * Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; * Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. * Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. * Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. * Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. * Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. * Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. * Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. * Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). * Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. * Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). * Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. * Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. * Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016. | SPEŁNIA TAK /NIE |
|  | Oprogramowanie bazodanowe | **Oprogramowanie Microsoft SQL Server Standard 2022 lub równoważne.**  Oraz 4 licencje CAL dwie licencje na użytkownika i 2 licencje na urządzenie, które zostanie przenaczone do wzmocnienia serwera utrzymującego dane systemów do inwentaryzacji aktywów oraz ewidencja sieci , oraz do zakupowanego systemu DLP  Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego do Microsoft SQL Server Standard Edition:   * Posiada wsparcie dla systemu operacyjnego Microsoft Windows Server 2016, Windows Server 2019, Windows Server 2022, do którego Zamawiający posiada prawa licencyjne * Zapewnia możliwość wykorzystania jako silnika relacyjnej, analitycznej lub wielowymiarowej bazy danych * Umożliwia dostęp do danych poprzez strukturalny język zapytań SQL * Posiada narzędzia do definiowania raportów i wykonywania analiz biznesowych * Posiada możliwość automatycznej aktualizacji i instalację wszelkich poprawek producenta oprogramowania * Zapewnia wysoką dostępność co najmniej jednej baz danych w instancji z wykorzystaniem replik na platformie, Windows Server 2016 lub Windows Server 2019 lub Windows Server 2022 do których Zamawiający posiada prawa licencyjne * Zapewnia możliwość uwierzytelnienia użytkowników i grup zarządzanych przez usługę Active Directory systemu Windows * Pozwala na odtworzenie zawartości bazy danych po awarii * Posiada mechanizm optymalizujący wykorzystanie pamięci operacyjnej * Posiada mechanizm optymalizujący czas dostępu do danych * Posiada mechanizm zarządzający optymalnym rozłożeniem danych na dyskach, w celu uzyskania lepszej wydajności rozwiązania * Zapewnia możliwość wykorzystania co najmniej 24 rdzeni procesora i co najmniej 128 GB pamięci RAM    Wymagania dodatkowe:  1. W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego, Wykonawca musi dowieść że dostarczane oprogramowanie spełnia wymagania funkcjonalne oraz musi być kompatybilne i w sposób niezakłócony działać w konfiguracji AlwaysOn Availability Groups wraz z oprogramowaniem Microsoft SQL Server funkcjonującym u Zamawiającego.  2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego, Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania oprogramowania równoważnego w środowisku sprzętowo-programowym Zamawiającego.  3. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.  4. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.  5. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.  6. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach. | **Producent**  **Nazwa I wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | Bezpieczeństwo | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). | SPEŁNIA TAK /NIE |
|  | Karta Zarządzania | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) | SPEŁNIA TAK /NIE |
|  | Oprogramowanie do zarządzania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | Oprogramowanie do monitorowania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Producenta dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android * Certyfikaty   + Oferowana platforma musi być zaprojektowana zgodnie ze standardami:     - ISO 27001     - NIST Security and Privacy Controls for Federal Information Systems and Organization     - CSA Cloud Control Matrix | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. | SPEŁNIA TAK /NIE |
|  | Dokumentacja użytkownika | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | SPEŁNIA TAK /NIE |
|  | Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego,  automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.  Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.  Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.  Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.  Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury.  Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :   * Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. * Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. * Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :   a. o poprawkach i usprawnieniach dotyczących aktualizacji  b. dacie wydania ostatniej aktualizacji  c. priorytecie aktualizacji  d. zgodność z systemami operacyjnymi  e. jakiego komponentu sprzętu dotyczy aktualizacja  f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.   * wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne * możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. * - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr ) * sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania ) * dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml * raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | Warunki gwarancji | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia Producenta/lub autoryzowanego Dystrybutora potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. | SPEŁNIA TAK /NIE |

## 8 SYSTEM NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO – 220 IP

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Dane producenta /model | Producent oferowanego rozwiązania /model i wersja modelu | **Producent:**    **Nazwa i wersja oprogramowania:** |
|  | Opis funkcjonalności rozwiązania | Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).  Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.  Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. | SPEŁNIA TAK /NIE |
|  | Wymagania ogólne rozwiązania NAC | 1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.  2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.  3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.  4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.  5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.  6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.  7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.  8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS  9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową  10.**Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę Vmware o Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 500 urządzeń.**  11. **Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 220 urządzeń wraz ze wsparciem technicznym na okres na minimum 12 m-cy** | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe – monitorowanie podsieci | 1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.  2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora  3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie  4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.  5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.  6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.  7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe – polityka bezpieczeństwa | 1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.  2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.  3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:  a. pełny dostęp  b. blokowanie (całkowity brak dostępu)  c. ograniczony dostęp  4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.  5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.  6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.  7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci. | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe – mechanizm kwarantanny | 1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa  2. Mechanizm kwarantanny powinien umożliwiać:  a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,  b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować  3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny  4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń  5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp  6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych  7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci  8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe – integracja z systemami zewnętrznymi | 1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD  2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.  3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.  4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.  5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.  6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal) | 1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.  2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.  3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory  4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń  5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych  6. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci  7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy  8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu  9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa  10.Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci  11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu  12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych  13.Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.  14.Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant  15.Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant | SPEŁNIA TAK /NIE |
|  | Pozostałe wymagania | 1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).  2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.  3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.  4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN  5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci | SPEŁNIA TAK /NIE |
|  | Usługi | Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania w siedzibie Zamawiającego:  - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego  - szkolenie dla administratora rozwiązania  - wsparcie w języku polskim w trybie 8x5 w dni robocze  - kwartalny przegląd konfiguracji rozwiązania  Wymaga się, aby dostawca przedstawił:  - oświadczenie Producenta lub Autoryzowanego Dystrybutora Producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia należy załączyć do oferty  - osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie , należy załączyć do oferty | SPEŁNIA TAK /NIE |
|  | Wsparcie | Wymaga się, aby dostawca zaoferował usługę zdalnego wsparcia w zakresie reagowania na raportowane przez NAC zdarzenia, przez okres minimum 24 miesięcy  - w trybie ciągłym 24/7, z czasem reakcji 4 godziny, w zakresie:  - odbieranie alertów mailowych wysyłanych przez NAC  - bieżąca analiza raportowanych zdarzeń pod kątem istniejącego zagrożenia bezpieczeństwa sieci  - natychmiastowe powiadamianie zespołu IT Zamawiającego w przypadku podejrzenia aktywnego zagrożenia i stwierdzenia konieczności szybkiej reakcji  - merytoryczne wsparcie w procesie reagowania na raportowane przez NAC zagrożenia  - okresowe sporządzanie podsumowań o zagrożeniach wykrytych z zaraportowanych przez NAC (co miesiąc)  - okresowe sporządzanie wykazu niezaufanych urządzeń, wykrytych przez NAC (co miesiąc)  - okresowe weryfikowanie skuteczności monitorowania sieci przez NAC, poprzez celowe i kontrolowane wywołanie zdarzeń (raz na kwartał)  - okresowe sprawdzanie dostępności aktualizacji i aktualizowanie oprogramowania NAC (co miesiąc)  Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. (dokumenty załączyć do oferty). | SPEŁNIA TAK /NIE |

## 9. SYSTEM DETEKCJI I REAKCJI NA ZDARZENIA W KOŃCOWYCH PUNKACH – EDR – 120 licencji

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum **12 miesięcy**.  Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. **12 miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).  Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.  Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.  Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.  Ilość licencji dla komputerów: **120 szt.** | SPEŁNIA TAK /NIE |
|  | **Ochrona punktów końcowych urządzeń komputerowych** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.  Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:   * + Microsoft Windows 10   + Microsoft Windows 11   + MacOS version 14 "Sonoma"   + MacOS version 13 "Ventura"   + MacOS version 12 "Monterey"   Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:   * + Microsoft Internet Explorer   + Microsoft Edge   + Mozilla Firefox   + Google Chrome   + Safari   Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej   1. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 2. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 3. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych. 5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 6. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:    * dostęp do pliku;    * tworzenie nowego procesu;    * nawiązane połączenia sieciowe;    * wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;    * zawartość skryptów uruchamianych na monitorowanej stacji. 7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 12. Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych. 14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym. 16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 19. Każda detekcja zawiera co najmniej następujące informacje:   • Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.  • Data i czas wystąpienia podejrzanych zdarzeń.  • Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.  • Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.  • Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.  • Poziom ryzyka, określający istotność danej detekcji.  • Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).   1. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 2. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 3. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 4. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 5. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 6. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 7. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 8. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 9. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 10. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 11. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 12. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 13. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 14. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 15. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim. 16. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji. 17. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 18. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR. 19. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 20. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware. 21. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) 22. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach. 23. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny. 24. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania. 25. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami. 26. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe. 27. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików. 28. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 29. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 30. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 31. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 32. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 33. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego. 34. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 35. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 36. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania. 37. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 38. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 39. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 40. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 41. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 42. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 43. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 44. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 45. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 46. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 47. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 48. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 49. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”. 50. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 51. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 52. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 53. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 54. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie. 55. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 56. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 57. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 58. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach. 59. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 60. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 61. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 62. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 63. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 64. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 65. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 66. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 67. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 68. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS. 69. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”. 70. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 71. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 72. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 73. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego. 74. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 75. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 76. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 77. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 78. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 79. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 80. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 81. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji. 82. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 83. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 84. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 85. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 86. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu. 87. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 88. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 89. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 90. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 91. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 92. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 93. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 94. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 95. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 96. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 97. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 98. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 99. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 100. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 101. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 102. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 103. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 104. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 105. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 106. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 107. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 108. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 109. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 110. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 111. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 112. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 113. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 114. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 115. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 116. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 117. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 118. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji. 119. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 120. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 121. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 122. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 123. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 124. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 125. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop). 126. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.   Centralna administracja   1. Portal zarządzający jest dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta. 4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami. 10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365. 22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji | **Producent:**    **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | **Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR)** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.  Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:  • Microsoft Windows 10  • Microsoft Windows 11  • MacOS 11 “Big Sur”  • MacOS 10.15 “Catalina”  • MacOS 10.14 “Mojave”  • MacOS 10.15 “Catalina”  Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:  • Microsoft® Windows Server 2012  • Microsoft® Windows Server 2016  • Microsoft® Windows Server 2019  • Microsoft® Windows Server 2022  Wspierane przeglądarki internetowe:  • Microsoft Edge  • Mozilla Firefox  • Google Chrome  • Safari  Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.  1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.  2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.  3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.  4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.  5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.  6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:  • dostęp do pliku;  • tworzenie nowego procesu;  • nawiązane połączenia sieciowe;  • wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;  • zawartość skryptów uruchamianych na monitorowanej stacji.  7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.  8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.  9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.  10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).  11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.  12. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.  13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.  14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.  15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.  16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.  17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.  18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.  19. Każda detekcja zawiera co najmniej następujące informacje:  • Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.  • Data i czas wystąpienia podejrzanych zdarzeń.  • Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.  • Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.  • Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.  • Poziom ryzyka, określający istotność danej detekcji.  • Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).  20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).  21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).  22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.  23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.  24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.  25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.  26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.  27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.  28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.  29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.  30. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.  31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.  32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.  33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.  34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.  35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.  36. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.  37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.  38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.  39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.  40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.  41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | **Certyfikaty i standardy** | * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/endpoint-protection-platforms>   minimalne wymaganie:  minimalna liczba referencji 65  minimalna ocena z referencji 4,6  (załączyć wydruk)   * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions>   minimalne wymaganie:  minimalna liczba referencji 17  minimalna ocena z referencji 4,4  (załączyć wydruk)  system musi posiadać certyfikaty:   * OPSWAT (dla EDR na poziomie min. Platinium), * AV Comperative Advance + * AV-TEST (ochrona w 2023 na poziomie min.6) * Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6 * producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem. | SPEŁNIA TAK /NIE |
|  | **Rozszerzone wsparcie serwisowe** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres **12** miesięcy.  System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Przygotowanie do zdalnej konfiguracji.  • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**  Oferent winien przedłożyć dokumenty:  • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. | SPEŁNIA TAK /NIE |

## 10. SYSTEM ZARZĄDZANIA INFORMACJAMI I ZDARZENIAMI BEZPIECZEŃSTWA INFORMATYCZNEGO - SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum **12 miesięcy**.  Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. **12 miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).  Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.  Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.  Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.  Ilość licencji dla hostów (IP adres ): **220 zt.** | SPEŁNIA TAK /NIE |
|  | **Zaawansowany skaner podatności** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym.  2. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania.  3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.  4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta  5. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych:  • Microsoft Edge  • Mozilla Firefox  • Google Chrome  • Safari  6. Konsola zarządzająca dostępna jest w języku polskim.  7. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.  8. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.  9. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).  10. Konsola wyposażona jest w panel kontrolny, w którym wyświetlane są informacje podsumowujące dotyczące poziomu bezpieczeństwa chronionej organizacji.  11. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania.  12. Ta sama konsola umożliwia zarządzanie innymi produktami w przypadku posiadania odpowiedniej licencji w tym co najmniej ochrony antymalware, systemem EDR, ochroną usług Microsoft 365  13. Konsola pozwala na podgląd posiadanych licencji oraz ich wykorzystania.  14. Oprogramowanie skanujące podatności bez agentowo (lokalny scan node) dostępne jest w postaci aplikacji instalowanej lokalnie i wspiera poniższe systemy operacyjne:  • Windows Server 2016 i nowsze  • Ubuntu server (wersje 64 bitowe 16.x 18.x, 20.x)  • Debian (wersje 64 bitowe 9,10,11)  15. Rozwiązanie umożliwia również agentowe skanowanie w poszukiwaniu podatności na komputerach z systemem Windows.  16. Agent instalowany na systemach Windows wspiera systemy MS Windows 10 i 11 oraz systemy serwerowe MS Windows Server 2016 i nowsze.  17. Ten sam agent zainstalowany na wspieranych systemach Windows w przypadku posiadania odpowiedniej licencji może dodatkowo zapewniać również ochronę antymalware i funkcjonalność systemu EDR.  18. Skanowanie agentowe odbywać się może w cyklach co:4,6,12,24 godzin  19. Istnieje możliwość włączenia i wyłączenia funkcji skanowania agentowego.  20. Wyłączenie funkcji skanowania agentowego nie powoduje deinstalacji agenta na danym hoście.  21. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.  22. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:  a) wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.  b) wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.  c) Pozwala na konfigurację parametrów skanowania takich jak:  a. zakres przeszukiwanych portów (osobne wartości dla TCP i UDP)  b. wydajność skanowania (6 poziomów),  c. liczbę jednoczesnych wątków skanowania (1,2,4,8,16,24,32)  d. możliwość wykrycia wersji systemu operacyjnego.  d) konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)  e) określenia maksymalnej ilości wykonanych skanowań (1-100) lub bez ograniczenia.  f) konfigurację wysyłania powiadomień na wskazane adresy e-mail  g) powiadomienia dotyczyć mogą: informacji o rozpoczęciu skanowania, jego zakończeniu, zmiany ilości hostów w stosunku do poprzedniego skanowania, zmiany ilości portów w stosunku do poprzedniego skanowania.  23. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.  24. Widok listy dostępnych skanowań wykrywających obiekty pozwala na zaawansowane filtrowanie.  25. Konsola pozwala na uruchomienie z poziomu listy dostępnych skanowań, wskazanego skanowania wykrywającego obiekty na żądanie z pominięciem harmonogramu.  26. Trwające zadanie skanowania w poszukiwaniu obiektów może zostać przerwane na żądanie.  27. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLSX oraz XML.  28. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.  29. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:  a) określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.  b) masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.  c) konfigurację parametrów skanowania, takich jak:  a. zakres skanowanych portów sieciowych TCP/UDP,  b. parametr wydajności skanowania (6 poziomów)  c. rodzaj uwierzytelniania na skanowanej stacji.  d) konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.  e) konfigurację wysyłania powiadomień na wskazane adresy e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.  30. W przypadku tworzonego zadania skanowania administrator posiada możliwość określenia czy do celu skanowania mają zostać wykorzystane wszystkie dostępne pluginy skanujące, tylko wybrane, wszystkie pluginy poza wskazanymi.  31. Administrator posiada możliwość podglądu dostępnych pluginów skanujących podatności i przeszukiwania ich listy.  32. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa.  33. Konsola pozwala na uruchomienie i zatrzymanie skanowania w poszukiwaniu znanych podatności na żądanie.  34. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku docx i xml  35. Dla danego hosta widoczne są wyniki skanowania w poszukiwaniu podatności.  36. Wyniki zawierają listę wykrytych podatności wraz z poziomem ich krytyczności  37. Dla danej wykrytej podatności dostępny jest: jej opis, poziom krytyczności w oparciu o punktację CVSS, datę wykrycia, wersję pluginu który wykrył podatność, sugestię rozwiązania (jeśli jest dostępna), informację o publicznie dostępnym exploicie (jeśli jest dostępna), zewnętrzne referencje (jeśli są dostępne).  38. Dla wybranych przez administratora wykrytych podatności, w celu ich obsługi istnieje możliwość stworzenia zgłoszenia we wbudowanym w rozwiązanie systemie zgłoszeń.  39. Podczas tworzenia zgłoszenia administrator ma możliwość określenia: nazwy zgłoszenia, wskazania konta osoby, do której zgłoszenie zostanie przypisane, priorytetu, tzw. „dedline” do którego zgłoszenie powinno zostać rozwiązane, dodatkowego opisu.  40. Lista wszystkich stworzonych zgłoszeń wraz z ich statusem widoczna jest z poziomu konsoli zarządzającej.  41. Administrator posiada możliwość sortowania oraz filtrowania stworzonych zgłoszeń.  42. Osoba, dla której zostało przypisane zgłoszenie ma możliwość dodawania komentarzy, w celu informowania o etapach procesu rozwiązywania zgłoszenia.  43. Dla zgłoszenia istnieje możliwość zmiany jego statusu.  44. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.  45. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:  a) określenie skanowanego celu za pomocą adresu URL.  b) konfigurację parametrów skanowania takich jak:  a. rodzaje testowanych ataków,  b. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),  c. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).  c) konfigurację uwierzytelniania w testowanej aplikacji web.  d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.  e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.  46. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych  47. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.  48. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:  a) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.  b) zapisywanie wskazanych warunków wyszukiwania jako szablony.  c) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.  d) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.    49. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.  50. Lista wszystkich wykrytych podatności musi umożliwiać:  a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (tag), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy.  b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.  c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.  51. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego.  52. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów  53. Raport podsumowujący umożliwia:  a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,  b) wybranie grup urządzeń, które będą znajdowały się w raporcie,  c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,  d) Utworzenie harmonogramu generowania raportu  e) Wskazanie adresu email na który zostanie wysłany link udostępniający wygenerowany raport, wraz z określeniem czasu ważności linku  54. Lista wygenerowanych raportów musi umożliwiać:  a) Wygenerowanie raportu na żądanie  b) eksport wyniku raportu do pliku XML(pogrupowany hostami), DOCX(pogrupowany hostami lub wykrytymi podatnościami lub podsumowujący), XLSX (pogrupowany wykrytymi podatnościami)  55. Administrator ma możliwość określenia: strefy czasowej dla swojej organizacji, długości przetrzymywania raportów (miesiąc, kwartał, pół roku, rok, 2 lata)  56. Dostęp do konsoli może być ograniczony na podstawie adresów IP lub ich zakresu. | **Producent:**    **Nazwa i wersja oprogramowania :**  SPEŁNIA TAK /NIE |
|  | **Usługa SIEM/SOC** | * Monitorowanie krytycznych wykryć skanera podatności oraz modułów EDR/XDR przez certyfikowanych ekspertów producenta oprogramowania * Walidacja i dochodzenie czy wykrycia są prawdziwe oraz czy wymagają natychmiastowej akcji by zatrzymać incydent, bądź czy są fałszywymi wykryciami * Eskalacja incydentu do adekwatnego reprezentanta klienta mającego możliwość i autorytet aby odpowiedzieć na incydent * Porada ekspertów jak zatrzymać i naprawić incydent – na przykład, rekomendując izolację systemów bądź zatrzymanie złośliwych procesów * Przygotowywanie raportów dla klienta wraz z sugestiami rozwiązań.   Zawartość raportu : Szczegóły raportu, Przegląd podatności, Podsumowanie podatności, Lista podatności (według podatności i hosta) z opcjami Wglądu, Podsumowania, Wykrywania, Odniesień i Ograniczenia tekstu do 500 znaków.  Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności  Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów w trybie miesięcznym (minimum raz w miesiącu). Raporty dostarczane kanałem e-mail lub w inny bezpieczny sposób komunikacji ustalony z Zamawiającym. | SPEŁNIA TAK /NIE |
|  | **Certyfikaty i standardy** | * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions>   minimalne wymaganie:  minimalna liczba referencji 17  minimalna ocena z referencji 4,4  (załączyć wydruk)  system musi posiadać certyfikaty:   * OPSWAT (dla EDR na poziomie min. Platinium), * AV Comperative Advance + * Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6 * producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem. | SPEŁNIA TAK /NIE |
|  | **Rozszerzone wsparcie serwisowe** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [**24**] miesięcy.  System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Przygotowanie do zdalnej konfiguracji.  • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać** **certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**  Oferent winien przedłożyć dokumenty:  • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. | SPEŁNIA TAK /NIE |

## 11. SYSTEM ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP) - 150 LICENCJI

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Parametr | Charakterystyka (wymagania minimalne) | Oferowane parametry |
|  | Architektura / budowa | 1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 150 Klientów jednocześnie.  1.2. Architektura / budowa:  1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.  1.2.1.1. Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.  1.2.1.2. Serwer i klient posiadają certyfikaty SSL (4096 bitowe).  1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).  1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.  1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.  1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.  1.3. Konfiguracja Architektury:  1.3.1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.  1.3.2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.  1.3.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy.  1.3.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.  Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku \*.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku \*.msi.  Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.  System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.  Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).  System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.  1.3.10. Klient musi mieć definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.  1.3.11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.  1.3.12 System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.  1.3.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów.  1.4. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.  1.4.1. Automaty powinny realizować co najmniej:  1.4.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych.  1.4.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. | **Producent:**    **Nazwa i wersja oprogramowania :**      SPEŁNIA TAK /NIE |
|  | Wymagania systemowe | 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).  2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.  2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2  2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.  2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java (JRE lub JDK), Apache Tomcat 8+.  2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).  2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. | SPEŁNIA TAK /NIE |
|  | Interfejsy | * 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.      1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.      2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.      3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.   2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.   3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.   4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.   5. System zapewnia integrację z modelem LLM. | SPEŁNIA TAK /NIE |
|  | Funkcjonalności systemu | 4.1. Funkcjonalność Klienta  4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).  4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików.  4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.  4.2. Funkcjonalność konsoli administracyjnej.  4.2.1. Konsola musi być w pełni polskojęzyczna.  4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).  4.2.3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.  4.2.4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.  4.2.5. Dane na widżetach muszą być aktualizowane automatycznie.  4.2.6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).  4.2.7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu.  4.2.8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.  4.2.9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.  4.2.10. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.  4.2.11. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).  4.2.12. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.  4.2.13. Konsola musi zawierać w sobie pełną dokumentację systemu.  4.3. Odczytywanie zainstalowanego oprogramowania  4.3.1. System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji.  4.4. Wzorce aplikacji i pakietów  4.4.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.  4.4.2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.  4.4.3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.  4.4.4. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.  4.5. Inwentaryzacja sprzętu komputerowego  4.5.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).  4.5.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.  4.5.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).  4.5.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.  4.5.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.  4.5.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).  4.5.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).  4.5.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.  4.5.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.  4.5.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).  4.5.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.  4.5.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.  4.5.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)  4.5.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu.  4.5.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).  4.5.15.1. System musi umożliwiać definiowanie typów serwisów  4.5.15.2. System musi umożliwiać definiowanie wartości serwisu  4.5.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji  4.5.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.  4.5.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).  4.6. Inwentaryzacja urządzeń podłączanych do komputera.  4.6.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)  4.6.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.  4.6.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).  4.7. Inwentaryzacja urządzeń sieciowych.  4.7.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.  4.7.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.  4.7.3. System musi zbierać informacje o jakości połączenia:  4.7.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach:  4.7.4.1. Średni czas odpowiedzi.  4.7.4.2. Minimalny czas odpowiedzi.  4.7.4.3. Maksymalny czas odpowiedzi.  4.7.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.  4.7.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.  4.7.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci  4.7.6.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.  4.7.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.  4.7.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.  4.7.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.  4.8. Zdalna administracja komputerami  4.8.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.  4.8.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.  4.8.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.  4.8.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).  4.8.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.  4.8.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów  4.8.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).  4.8.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)  4.8.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.  4.8.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota~~/NIE~~dziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.  4.8.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.  4.8.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.  4.8.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.  4.8.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).  4.8.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).  4.8.3.1. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.  4.8.3.2. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.  4.8.3.3. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).  4.8.4. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.  4.8.5. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.  4.9. Wysyłanie wiadomości  4.9.1. Komunikator  4.9.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.  4.9.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora.  4.9.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.  4.9.1.4. System musi przechowywać historię konwersacji.  4.9.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.  4.9.2. Wiadomość Jednorazowa:  4.9.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.  4.9.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.  4.9.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.  4.9.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników.  4.9.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.  4.9.3. Wiadomości Cykliczne:  4.9.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.  4.9.3.2. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.  4.9.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.  4.9.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.  4.9.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.  4.9.4. System szkolenia pracowników za pomocą wiadomości.  4.9.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.  4.9.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.  4.9.4.3. Formatowanie treści musi być zgodne z HTML.  4.9.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).  4.9.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.  4.9.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.  4.9.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.  4.9.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.  4.9.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).  4.10. Repozytorium CMDB  4.10.1.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta.  4.11. Worktime manager  4.11.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.  4.11.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.  4.11.3. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.  4.12. Zarządzanie politykami bezpieczeństwa.  4.12.1. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.  4.12.2. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.  4.12.3. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).  4.12.4. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.  4.12.5. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.  4.12.6. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych.  4.12.7. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.  4.12.8. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną  4.12.9. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.  4.12.10. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).  4.12.11. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.  4.12.12. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.  4.12.13. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.  4.12.14. System musi mieć możliwość określenia ram czasowych działania danej reguły.  4.12.15. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.  4.13. System musi w pełni wspierać następujące polityki ochrony danych:  4.13.1. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.  4.13.2. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu.  4.13.3. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym.  4.13.4. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.  4.13.5. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).  5. Kontrola i ochrona urządzeń  5.1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.  5.2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzań USB.  5.3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.  5.3.1. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.  6. Klasyfikacja i ochrona dokumentów  6.1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.  6.2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.  6.3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.  7. Szyfrowanie dysków  7.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS\_AES\_256 i AES\_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.  8. Ochrona danych w użyciu  8.1. Podjęcie działania w momencie uruchomienia określonego procesu.  8.2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.  9. Ochrona danych w ruchu  9.1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów.  9.2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.  10. Raportowanie i eksport danych  10.1. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.  10.2. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.  10.3. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.  10.4. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).  10.5. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.  11. Bezpieczeństwo  11.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.  11.1.1. Uwierzytelnianie do systemu musi być realizowane:  11.1.1.1. z wykorzystaniem imiennego konta użytkownika i hasła,  11.1.1.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,  11.1.1.3. za pośrednictwem uwierzytelniania poprzez Active Directory,  11.1.1.4. za pośrednictwem uwierzytelniania poprzez CAS,  11.1.2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.  11.1.3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).  11.1.4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).  11.1.4.1. Uwierzytelnianie z wykorzystaniem obrazu wideo.  11.1.4.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika.  11.1.4.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.  11.1.5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.  11.1.5.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10/11 i Windows Server 2012/2016/2019/2022.  11.1.6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:  11.1.6.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.  11.1.6.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.  11.1.7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.  11.1.8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.  11.1.8.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.  11.1.9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.  11.1.10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.  11.1.11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.  11.1.12. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.  11.1.13. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).  11.1.14. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.  11.1.15. System musi zapewniać:  11.1.15.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.  11.1.15.2. Przechowywanie logów systemowych.  11.1.15.3. Przechowywanie logów bezpieczeństwa.  11.1.15.4. Przechowywanie logów aktywności użytkowników i administratorów.  11.1.15.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.  11.1.15.6. Możliwość eksportu logów.  11.1.15.7. Definiowanie maksymalnego czasu przechowywania plików log.  11.1.15.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.  11.1.15.9. Definiowanie ścieżki do kopii zapasowej  11.1.15.10. Definiowanie ścieżki do importu danych  11.1.15.11. Definiowanie ścieżki do zapisu raportów  11.1.15.12. Definiowanie serwera do importu danych | SPEŁNIA TAK /NIE |
|  | Wsparcie i pomoc | 12.1.1 System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinariów w języku polskim.  12.1.2 System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.  12.1.3 Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.  12.1.4. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.   1. Czas trwania usługi SLA wynosi 12 miesiecy od dnia zakupu  Usługi Utrzymania Oprogramowania obejmują: 2. asystę techniczną, 3. świadczenie usług SLA, w ramach, których realizowana jest: 4. obsługa zgłoszeń w zakresie: -reakcja na zgłoszenia błędów w określonym czasie reakcji; -dokonywanie analizy przyczyn błędów; 5. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich; 6. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego; 7. usuwania błędów w czasie naprawy; 8. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy; 9. zapewnienia dostępności Oprogramowania. | SPEŁNIA TAK /NIE |
|  | Gwarancja | Minimum 12 -mcy | SPEŁNIA TAK /NIE |
|  | Wdrożenie | 1. Wdrożenie realizowane jest bezpośrednio przez Producenta oprogramowania, 2. Wdrożenie realizowane jest w formie zdalnej, 3. Komunikacja musi odbywać się w języku polskim, 4. Wdrożenie obejmuje pełną konfigurację wszystkich modułów niezbędnych do uruchomienia systemu 5. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania zakończone certyfikatem dla administratora systemu wystawionym bezpośrednio przez producenta oprogramowania | SPEŁNIA TAK /NIE |

## 12. OPROGRAMOWANIE ANTYWIRUSOWE DEDYKOWANE DO SERWERÓW- 15 licencji

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum **12 miesięcy**.  Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. **12 miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).  Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.  Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.  Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.  Ilość licencji dla komputerów: **15 szt.** | SPEŁNIA TAK /NIE |
|  | **Ochrona serwerów** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.  Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:  • Microsoft Windows Server 2016  • Microsoft Windows Server 2019  • Microsoft Windows Server 2022  Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:  • Microsoft Edge  • Mozilla Firefox  • Google Chrome  • Safari  Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:  Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej   1. Oprogramowanie instalowane na serwerach , zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach . 5. Dane zebrane przez agenta instalowanego na serwerach są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:    * dostęp do pliku;    * tworzenie nowego procesu;    * nawiązane połączenia sieciowe;    * wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;    * zawartość skryptów uruchamianych na monitorowanej stacji. 7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 8. Dane zbierane przez agenta instalowanego na serwerach , przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych. 14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym. 16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 19. Każda detekcja zawiera co najmniej następujące informacje:   • Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.  • Data i czas wystąpienia podejrzanych zdarzeń.  • Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.  • Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.  • Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.  • Poziom ryzyka, określający istotność danej detekcji.  • Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).   1. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 2. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 3. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 4. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 5. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 6. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 7. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 8. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 9. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 10. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 11. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 12. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 13. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 14. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 15. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim. 16. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji. 17. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 18. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR. 19. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 20. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware. 21. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) 22. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach. 23. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny. 24. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania. 25. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami. 26. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe. 27. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików. 28. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 29. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 30. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 31. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 32. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 33. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego. 34. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 35. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 36. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania. 37. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 38. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 39. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 40. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 41. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 42. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 43. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 44. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 45. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 46. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 47. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 48. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 49. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”. 50. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 51. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 52. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 53. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 54. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie. 55. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 56. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 57. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 58. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach. 59. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 60. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 61. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 62. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 63. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 64. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 65. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 66. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 67. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 68. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS. 69. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”. 70. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 71. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 72. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 73. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego. 74. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 75. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 76. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 77. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 78. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 79. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 80. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 81. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji. 82. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 83. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 84. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 85. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 86. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu. 87. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 88. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 89. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 90. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 91. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 92. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 93. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 94. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 95. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 96. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 97. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 98. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 99. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 100. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 101. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 102. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 103. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 104. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 105. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 106. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 107. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 108. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 109. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 110. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 111. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 112. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 113. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 114. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 115. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 116. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 117. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 118. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji. 119. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 120. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 121. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 122. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 123. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 124. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 125. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop). 126. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.   Centralna administracja   1. Portal zarządzający jest dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta. 4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami. 10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365. 22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji | **Producent:**    **Nazwa i wersja oprogramowania** |
|  | **Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR)** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.  Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:  • Microsoft Windows 10  • Microsoft Windows 11  • MacOS 11 “Big Sur”  • MacOS 10.15 “Catalina”  • MacOS 10.14 “Mojave”  • MacOS 10.15 “Catalina”  Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:  • Microsoft® Windows Server 2012  • Microsoft® Windows Server 2016  • Microsoft® Windows Server 2019  • Microsoft® Windows Server 2022  Wspierane przeglądarki internetowe:  • Microsoft Edge  • Mozilla Firefox  • Google Chrome  • Safari  Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.    1. Oprogramowanie instalowane na serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.  2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.  3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.  4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach.  5. Dane zebrane przez agenta instalowanego na serwerach są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.  6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:  • dostęp do pliku;  • tworzenie nowego procesu;  • nawiązane połączenia sieciowe;  • wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;  • zawartość skryptów uruchamianych na monitorowanej stacji.  7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.  8. Dane zbierane przez agenta instalowanego na serwerach , przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.  9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.  10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).  11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.  12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.  13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.  14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.  15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.  16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.  17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.  18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.  19. Każda detekcja zawiera co najmniej następujące informacje:  • Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.  • Data i czas wystąpienia podejrzanych zdarzeń.  • Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.  • Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.  • Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.  • Poziom ryzyka, określający istotność danej detekcji.  • Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).  20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).  21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).  22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.  23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.  24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.  25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.  26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.  27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.  28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.  29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.  30. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.  31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.  32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.  33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.  34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.  35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.  36. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.  37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.  38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.  39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.  40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.  41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA TAK /NIE |
|  | **Certyfikaty i standardy** | * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/endpoint-protection-platforms>   minimalne wymaganie:  minimalna liczba referencji 65  minimalna ocena z referencji 4,6  (załączyć wydruk)   * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions>   minimalne wymaganie:  minimalna liczba referencji 17  minimalna ocena z referencji 4,4  (załączyć wydruk)  system musi posiadać certyfikaty:   * OPSWAT (dla EDR na poziomie min. Platinium), * AV Comperative Advance + * AV-TEST (ochrona w 2023 na poziomie min.6) * Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6 * producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem. | SPEŁNIA TAK /NIE |
|  | **Rozszerzone wsparcie serwisowe** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres **12** miesięcy.  System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Przygotowanie do zdalnej konfiguracji.  • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**  Oferent winien przedłożyć dokumenty:  • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. | SPEŁNIA TAK /NIE |

## 13 WDROŻENIE I SZKOLENIE

## A WDROŻENIE SERWERA WIRTUALIZACYJNEGO Z SYTEMEM BAZODANOWYM i BIBLIOTEKI TAŚMOWEJ

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Analiza Przedwdrożeniowa | - Audyt Infrastruktury :  - Przeprowadzenie kompleksowego audytu aktualnej infrastruktury, w tym analizy sprzętu, oprogramowania, sieci oraz polityki bezpieczeństwa.  - Identyfikacja Wymagań :  - Konsultacje z kluczowymi interesariuszami w celu określenia wymagań technicznych i operacyjnych.  - Zdefiniowanie wymagań funkcjonalnych i niefunkcjonalnych dotyczących systemu serwerowego. | SPEŁNIA TAK /NIE |
|  | **Cel** | Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych , podłączenie do obecnej infrastruktury, konfiguracja urządzeń , zgodna z Zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów.  Wdrożenie serwera musi zostać przeprowadzone przez inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania. Wykonawca , przedłoży certyfikat , potwierdzający , ukończenie szkolenia instalacji i wdrożeń serwerów oferowanego producenta .  Szkolenie przeprowadzone powinno być , przez inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania systemu serwerowego . Wykonawca , przedłoży certyfikat , potwierdzający , ukończenie szkolenia  **Czas trwania szkolenia powinien potrwać nie mniej niż 10 godzin .** | SPEŁNIA TAK /NIE |
|  | Projekt Architektury Systemu | Opracowanie szczegółowego projektu architektury systemu Windows Server 2022, uwzględniającego strukturę sieci, role serwera, mechanizmy zabezpieczeń i zarządzania. | SPEŁNIA TAK /NIE |
|  | Wdrożenie Systemu | **1. Opis przedmiotu zamówienia**  **Przedmiotem zamówienia jest wdrożenie dwóch zaawansowanych przełączników sieciowych w infrastrukturze Zamawiającego, z kluczowym celem utworzenia stosu (stack) w celu zwiększenia wydajności i niezawodności sieci. Przełączniki mają zostać połączone w stos za pomocą dedykowanych kabli o długości 1 metra, co umożliwi scentralizowane zarządzanie oraz poprawi skalowalność sieci.**  **2. Zakres prac:**  **2.1. Dostawa i instalacja sprzętu:**  **Dostawa przełączników do lokalizacji wskazanej przez Zamawiającego.**  **Instalacja fizyczna: Montaż przełączników w istniejących szafach rackowych, uwzględniająca montaż urządzeń, podłączenie do systemu zasilania awaryjnego (UPS) oraz połączenie z istniejącą infrastrukturą sieciową.**  **2.2. Konfiguracja stosu (stacku):**  **Agregacja przełączników w stos: Połączenie obu przełączników za pomocą dedykowanego kabla o długości 1 metra, tworząc pojedynczy, logiczny przełącznik z centralnym punktem zarządzania.**  **Konfiguracja master/slave: Ustalenie hierarchii przełączników w stosie, z przypisaniem roli urządzenia nadrzędnego (master) oraz podrzędnego (slave).**  **Synchronizacja konfiguracji: Zastosowanie konfiguracji globalnej, aby ustawienia dotyczące VLAN-ów, routingu oraz polityk bezpieczeństwa były identyczne na wszystkich urządzeniach w stosie.**  **2.3. Konfiguracja sieciowa:**  **Konfiguracja VLAN-ów: Stworzenie i konfiguracja VLAN-ów zgodnie z wymaganiami Zamawiającego, w tym VLAN-ów dedykowanych dla różnych segmentów sieci (np. administracji, serwerów, gości).**  **Routing między VLAN-ami: Umożliwienie routingu między VLAN-ami w celu zapewnienia bezpiecznej i wydajnej komunikacji między różnymi segmentami sieci.**  **Implementacja redundancji: Wdrożenie mechanizmów redundancji sieciowej poprzez konfigurację protokołów, które zapewniają nieprzerwane działanie sieci w przypadku awarii jednego z przełączników.**  **2.4. Testowanie i weryfikacja:**  **Testy funkcjonalne: Przeprowadzenie testów mających na celu weryfikację poprawności działania skonfigurowanego stosu, w tym synchronizacji przełączników oraz poprawności funkcjonowania sieci po ich połączeniu.**  **Testy wydajnościowe: Przeprowadzenie testów przepustowości oraz szybkości przełączania, aby zapewnić optymalne działanie sieci w warunkach produkcyjnych.**  **Testy awaryjne: Sprawdzenie skuteczności redundancji poprzez symulację awarii jednego z przełączników i weryfikację, czy sieć nadal funkcjonuje bez przerw.**  **Zamawiający zastrzega sobie prawo do monitorowania postępu realizacji zamówienia oraz do wprowadzania zmian wynikających z potrzeb technicznych lub organizacyjnych.** | SPEŁNIA TAK /NIE |
|  |  | **1. Przedmiot zamówienia**  Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja systemu obejmującego bibliotekę taśmową. System ma zostać zainstalowany w infrastrukturze serwerowej Zamawiającego, spełniając określone wymagania techniczne i funkcjonalne.  **2. Zakres zamówienia**  Zakres zamówienia obejmuje:  **Dostawa sprzętu:** Dostarczenie biblioteki taśmowej zgodnej z wymaganiami technicznymi opisanymi w niniejszym OPZ.  **Instalacja fizyczna:**   * + Montaż biblioteki taśmowej w szafie rackowej 19-calowej, zgodnie z dostarczonymi szynami montażowymi.   + Podłączenie do zasilania awaryjnego (UPS) oraz do infrastruktury sieciowej Zamawiającego za pomocą odpowiednich interfejsów (np. SAS, Fibre Channel).   **Konfiguracja oprogramowania:**   * + Instalacja i konfiguracja oprogramowania do zarządzania biblioteką taśmową na serwerze lub stacji roboczej Zamawiającego.   + Ustawienie slotów, napędów oraz partycji w bibliotece taśmowej zgodnie z wymaganiami użytkownika.   + Przeprowadzenie testów funkcjonalnych oraz kalibracji.   **Szkolenie:**   * + Przeprowadzenie szkolenia dla zespołu IT Zamawiającego, obejmującego zarządzanie urządzeniem, podstawy obsługi, procedury konserwacji oraz procedury awaryjne. | SPEŁNIA TAK /NIE |
|  | Szkolenie | Zakres Szkolenia: Microsoft Windows Server 2022  1. Wprowadzenie do Windows Server 2022  Przegląd nowości i kluczowych funkcji Windows Server 2022.  Wymagania systemowe i instalacyjne.  Edycje Windows Server 2022 i ich zastosowania.  2. Instalacja i Konfiguracja  Przygotowanie środowiska do instalacji.  Proces instalacji krok po kroku.  Podstawowa konfiguracja po instalacji.  3. Zarządzanie Tożsamościami i Dostępem  Active Directory Domain Services (AD DS): Instalacja i konfiguracja.  Zarządzanie użytkownikami, grupami i jednostkami organizacyjnymi.  Polityki grup (Group Policy): Tworzenie, wdrażanie i zarządzanie.  4. Zarządzanie Zasobami Sieciowymi  Konfiguracja ról serwera: DNS, DHCP, File and Storage Services.  Zarządzanie udostępnianiem plików i drukarek.  Konfiguracja i zarządzanie systemem plików oraz przestrzenią dyskową.  5. Wirtualizacja z Hyper-V  Wprowadzenie do Hyper-V.  Instalacja i konfiguracja Hyper-V.  Zarządzanie maszynami wirtualnymi, sieciami wirtualnymi i przechowywaniem.  6. Bezpieczeństwo i Ochrona Danych  Zabezpieczenia w Windows Server 2022: BitLocker, Windows Defender, Firewall.  Zarządzanie aktualizacjami i poprawkami (Windows Update).  Kopie zapasowe i odzyskiwanie danych.  7. Monitorowanie i Optymalizacja Systemu  Narzędzia monitorowania systemu: Performance Monitor, Event Viewer.  Optymalizacja wydajności serwera.  Zarządzanie zasobami i wydajnością.  8. Automatyzacja i Zarządzanie Konfiguracją  Wprowadzenie do PowerShell i jego zastosowania.  Automatyzacja zadań administracyjnych za pomocą skryptów PowerShell.  Wprowadzenie do Windows Admin Center.  9. Scenariusze Zaawansowane  Wdrażanie i zarządzanie serwerami w chmurze (Azure).  Integracja Windows Server 2022 z usługami chmurowymi.  Zaawansowane scenariusze backupu i odzyskiwania. | SPEŁNIA TAK /NIE |

## B WDROŻENIE I SZKOLENIE SERWERA NAS

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **Wdrożenie** | Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych , podłączenie do obecnej infrastruktury, konfiguracja urządzeń , zgodna z Zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów NAS złożonego z 11 modułów. Szkolenie musi zostać **przeprowadzone przez certyfikowanego inżyniera** posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania. **Czas trwania szkolenia powinien potrwać nie mniej niż 30 godzin.** | SPEŁNIA TAK /NIE |
|  | **Szkolenie** | 1. **Zarządzanie przechowywaniem.** 2. Omówienie dostępnych typów RAID, ich specyfikacji, algorytmu działania, a także dobór najlepszego wariantu adekwatnie do przedstawionych wymagań. Szczegółowe omówienie tradycyjnych typów RAID takich jak RAID 1, 5, 6, 10 oraz niestandardowych SHR, SHR-2 i F1. 3. Omówienie dostępnych systemów plików, ich specyfikacji, funkcjonalności oraz architektury, a także dobór najlepszego wariantu do przedstawionych wymagań. 4. Omówienie specyfikacji dysków HDD i SSD kompatybilnych z posiadanym serwerem NAS pod kątem zastosowania w długoterminowym przechowywaniu danych. Objaśnienie różnic w mechanizmie zapisu na dyskach talerzowych oraz flash’owych. 5. Wpływ kluczowych parametrów SMART na działanie dysków w macierzy. 6. Procedura wymiany uszkodzonego dysku w grupie RAID. Rozbicie tematu na różne przypadki wraz z symulacją awarii. Wady i zalety stosowania dysków zapasowych. 7. Dostępne opcje rozbudowy istniejącej puli pamięci oraz ograniczenia z nimi związane z podziałem na zastosowane typy RAID. 8. Możliwości skalowalności urządzenia pod kątem zastosowania większej ilości dysków, a co za tym idzie zwiększenia pojemności istniejącej puli pamięci lub utworzenia nowej. 9. Wybór odpowiedniego priorytetu synchronizacji grupy RAID zależenie od zastosowanych dysków i przeznaczenia serwera NAS. Analiza obciążenia systemu i wykorzystania dysków przy jednoczesnym wykorzystywaniu zasobów serwera przez stacje klienckie. 10. Omówienie rodzajów testów SMART, ich cech charakterystycznych, przeznaczenia oraz przypadków zastosowania. Implementacja sensownego i bezpiecznego harmonogramu wykonywania testów, pełna automatyzacja poprzez dedykowane skrypty. 11. Dostępne mechanizmy wpływające na zwiększenie szybkości odczytu i zapisu danych, wymagania związane z implementacją takiego rozwiązania, wady i zalety zależenie od rodzaju środowiska serwerowego i wykorzystywanych aplikacji. Analiza żywotności wybranych nośników, symulacja czasu pracy oraz retencji w celu utrzymania najwyższego poziomu wydajności pamięci podręcznej w danej jednostce czasu z uwzględnieniem szacunkowych ilości zapisu i odczytu danych. 12. Algorytm szyfrowania danych – praktyczne zastosowanie, wpływ na obciążenie serwera i wydajność systemu, możliwości wykorzystania szyfrowania na różnego typu zasobach. Ograniczenia związana z włączeniem szyfrowania, zagrożenia wynikające z niezastosowania takiego algorytmu. 13. Kopiowanie przy zapisie (ang. copy on write) – zasada działania na przykładzie systemu plików btrfs. Zastosowanie praktyczne, wady i zalety, ograniczenia i wymagania. 14. **Użytkownicy i grupy.** 15. Zarządzanie użytkownikami i grupami lokalnymi, konfiguracja strategii bezpiecznego logowania, automatyzacja procesu tworzenia nowych użytkowników i wdrażania ich do korzystania z systemu. 16. Zarządzanie użytkownikami i grupami domenowymi, podłączanie serwera NAS jako klienta domeny, a także tworzenie niezależnego kontrolera domeny opartego o natywne rozwiązanie dostępne w systemie operacyjnym serwera NAS. Pełne wdrożenie testowe z uwzględnieniem zarządzania kontrolerem domeny w sposób rozszerzony poprzez dodatek RSAT, konfigurację profili mobilnych dla użytkowników domenowych z wykorzystaniem zasobów magazynowych serwera NAS. Konfiguracja polis związanych z automatyczną instalacją wskazanych programów na systemach klienckich. 17. Omówienie zasad nadawania uprawnień użytkownikom i grupom z wyszczególnieniem podziału na uprawnienia Unix i ACL. Implementacja obu wariantów w celu wyboru najbardziej odpowiedniego do postawionych wymagań. 18. **Foldery współdzielone.** 19. Zasada funkcjonowania folderów współdzielonych w systemie operacyjnym. Powiązanie z systemem plików działającym na podstawie wolumenów. 20. Omówienie działania systemu plików btrfs pod kątem utrzymania integralności danych z wykorzystaniem dodatkowych sum kontrolnych. 21. Wskazanie i wyjaśnienie algorytmu wykorzystywanego do kompresji danych. Wykorzystanie praktyczne wraz z testami oszczędności zajmowanej przez pliki przestrzeni po włączeniu kompresji. 22. Szczegółowe wytłumaczenie funkcjonalności WORM (ang. Write Once Read Many) działającej na poziomie folderów współdzielonych. Przykłady wykorzystania praktycznego oraz korzyści z tego płynące. 23. Foldery domowe – zasada funkcjonowania dla użytkowników lokalnych i domenowych. 24. Metody udostępniania plików osobom z zewnątrz z zachowaniem zasad bezpieczeństwa tj. szyfrowania transferu oraz zabezpieczenia dostępu przed osobami nieuprawnionymi. 25. **Ustawienia sieciowe.** 26. Zasada działania więcej niż dwóch interfejsów LAN w serwerze. Wyjaśnienie domyślnej adresacji LAN oraz przykładowa konfiguracja w sieci LAN bez serwera DHCP. 27. Agregacja łączy ze szczegółowym omówieniem specyfikacji każdego dostępnego trybu dedykowanego dla przełączników bez interfejsu zarządzania oraz dla tych z interfejsem zarządzania i wsparciem dla protokołu LACP (ang. Link Aggregation Control Protocol), standard 802.3ad. 28. Statyczny routing po stronie serwera NAS, ustawienia zasad filtrowania ruchu i sterowania ruchem z podziałem na konkretne usługi i porty. 29. Konfiguracja podstawowych parametrów połączeniowych serwera NAS z siecią Internet. Wyjaśnienie zasady działania takiego połączenia w momencie korzystania z kilku interfejsów LAN. Wady i zalety zamiennego stosowania nazwy serwera do połączeń CIFS/SMB zamiast adresu IP. 30. Zasada działania serwera proxy i przykład wykorzystania w realnym środowisku. 31. Konfiguracja niestandardowych portów zarządzania. Wyszczególnienie dostępnych metod lokalnego i zdalnego zarządzania serwerem poprzez interfejs Web UI oraz linię komend. 32. **Kopie zapasowe i ochrona danych.** 33. Zasady bezpiecznego przechowywania danych z przykładem implementacji w omawianym środowisku. 34. Metody wykonywania kopii zapasowej z uwzględnieniem różnego typu nośników tj. dysków USB, obudów RAID, bibliotek LTO, innych serwerów fizycznych oraz serwerów NAS. 35. Szczegółowe omówienie metod replikacji danych na inny serwer NAS tego samego producent oraz porównanie procesu do replikacji na inne rozwiązanie firmy trzeciej. Wskazanie najlepszej dostępnej metody do wykorzystania w sieci LAN oraz poprzez WAN. 36. Wyjaśnienie zasady działania mechanizmy migawek z wykorzystaniem kopiowania przy zapisie. Przedstawienie możliwości implementacji harmonogramu wykonywania migawek w systemie oraz związanych z tym najlepszych praktyk. Analiza potencjalnego wykorzystania przestrzeni przez migawki w długoterminowym procesie ich przechowywania oraz omówienie dostępnych strategii retencji wersji. 37. Metody odzyskiwania danych z migawek z opcją przywracania lokalnego oraz zdalnego. Wyjaśnienie różnic i cech szczególnych obu metod. 38. Utworzenie i przedstawienie w praktyce zasady działania replikacji migawek z uwzględnieniem przełączania awaryjnego między serwerami. Szczególnie w przypadku podłączenia do kontrolera domeny i odtwarzania danych wraz z uprawnieniami na serwerze docelowym. 39. Przedstawienie sposobów wykonywania kopii zapasowych do środowisk chmurowych. 40. **Klaster wysokiej dostępności.** 41. Omówienie wymagań dotyczących utworzenia klastra wysokiej dostępności z dwóch takich samych serwerów NAS. 42. Omówienie wymagań i ograniczeń dotyczących utworzenia klastra wysokiej dostępności z dwóch różnych serwerów NAS. 43. Zasada działania klastra SHA (ang. Synology High Availability). Wady I zalety oraz korzyści płynące z zastosowania rozwiązania klastrowego jako główne miejsce składowania danych i różnego typu usług. 44. Algorytm przełączania awaryjnego serwerów w klastrze. Jakie wymagania musi spełniać połączenie między serwerami, jakie ograniczenia występują, jakie problemy mogą wystąpić oraz jak w praktyce odczuwalna będzie praca na zasobach klastra SHA. 45. **Kopie zapasowe komputerów, serwerów i maszyn wirtualnych.** 46. Omówienie dostępnych metod wykonywania kopii zapasowych komputerów PC z zaprezentowaniem działania w praktyce z podziałem na kopie plikowe oraz bare-metal. 47. Opracowanie systemu wdrażania odpowiedniego rozwiązania do kopii zapasowej na dużą skalę. 48. Metody przywracania danych dostępne dla zwykłych użytkowników oraz administratorów. Praktyczne zastosowanie oraz instruktarz dotyczący każdej z dostępnych metod na przykładzie komputera z systemem Windows oraz Linux. 49. Możliwości masowego konfigurowania zasad tworzenia kopii zapasowych. 50. Wyjaśnienie i zaprezentowanie realnego wpływy szyfrowania i kompresji transferu danych na komputery lokalne. 51. Strategie przechowywania danych kopii zapasowych w planie długoterminowym z możliwością przywrócenia kopii zapasowej sprzed 6, 12, i 18 miesięcy. 52. Kontrola integralności danych kopii zapasowych i testowe odtwarzanie. 53. Możliwości automatyzacji procesu odtwarzania danych w przypadku awarii komputera. 54. Testowe przywracanie obrazu kopii w formie maszyny wirtualnej w natywnym wirtualizatorze dostępnym na serwerze NAS oraz na zewnętrznych wirtualizatorach. 55. Omówienie różnic w działaniu środowisk wirtualizacji opartych o KVM oraz QEMU. 56. Wyjaśnienie mechanizmów wpływających na redukcję zajmowanej przez kopie zapasowe przestrzeni takich jak deduplikacja i kompresja. Wykazanie algorytmu działania oraz wpływu na żywotność dysków. 57. Przedstawienie metody replikacji centralnego repozytorium kopii zapasowych na zapasowy serwer NAS z opcją przełączenia klientów na tę jednostkę i wznowienia harmonogramów kopii zapasowych. 58. Metody wykonywania kopii zapasowych systemów bazodanowych działających na serwerach fizycznych z systemami operacyjnymi z rodziny Windows oraz Linux oraz adekwatne metody przywracania. 59. Wykonywanie kopii zapasowych maszyn wirtualnych z różnych środowisk wirtualizacji obsługiwanych przez zintegrowane narzędzie dostępne w systemie serwera NAS. Wyjaśnienie zasady działania mechanizmu kopii, opcji przywracania natychmiastowego oraz pełnego. 60. **Serwer poczty.** 61. Omówienie dostępnych pakietów pozwalających na uruchomienie serwera pocztowego. Jakie są kluczowe różnice, plan licencjonowania, wady i zalety. 62. Wytypowanie odpowiedniego pakietu pozwalającego na utworzenie serwera pocztowego i na jego przykładzie zaprezentowanie praktycznego działania. 63. Wymagania dotyczące utworzenia serwera. 64. Wyjaśnienie zarządzania domeną oraz rekordami DNS. 65. Przekierowywanie portów wymaganych do działania usług na serwerze NAS. Niebezpieczeństwo płynące z tego typu praktyk. 66. Pełnoprawne uruchomienie serwera pocztowego po przeprowadzonej konfiguracji. Testy działania usług SMTP, IMAP i POP3. 67. Obsługa kont pocztowych za pomocą natywnego klienta oraz oprogramowania firm trzecich. 68. Monitorowanie stanu serwera pocztowego, potencjalnych zagrożeń, filtrowanie poczty oraz włączanie silników antyspamowych. 69. Praktyczne zaprezentowanie procedury migracji danych z istniejącego serwera pocztowego na nowe rozwiązanie zaimplementowane na serwerze NAS. 70. **System monitoringu.** 71. Omówienie wymagań związanych z wdrożeniem systemu monitoringu opartego o serwer NAS z centralnym zarządzaniem podległymi serwerami nagrywającymi. 72. Prezentacja funkcjonalności i zarządzania takim systemem w praktyce z wykorzystaniem co najmniej dwóch różnego typu kamer IP. Minimum jedna standardowa i jedna sterowana (ang. PTZ). 73. Konfiguracja przestrzeni przechowywania nagrań. Najlepsza dopuszczalna strategia retencji. 74. Analiza wydajności zapisu z wykorzystaniem systemów plików ext4 i btrfs. Wybór odpowiedniego rozwiązania pod kątem najlepszych osiągów. 75. Dodawanie różnego typu kamer do systemu monitoringu – kompatybilnych oraz z wykorzystaniem protokołu ogólnego ONVIF. 76. Przetestowanie działania wykrywania ruchu i innych podobnych funkcjonalności na poziomie zarządzania kamery oraz systemu monitoringu. 77. Automatyzacja dotycząca powiadamiania o zaistniałych zdarzeniach wykrytych przez system monitoringu. 78. Sposoby na redukcję przestrzeni zajmowanej przez nagrania, archiwizacja oraz tworzenie tzw. timelapse’ów. 79. Zarządzanie systemem. 80. Zarządzanie serwerem NAS i systemem operacyjnym pracującym na nim poprzez centralny system zarządzania, a także aplikacje mobilne. Wyszczególnienie ograniczeń i wymagań dotyczących każdej metody. 81. Zabezpieczenie serwera poprzez wdrożenie zasada automatycznego blokowania adresów IP, białej oraz czarnej listy, filtrowania ruchu przychodzącego. 82. Wdrożenie uwierzytelniania dwuskładnikowego dla użytkowników posiadających zdalny dostęp do zarządzania serwerem. 83. Konfiguracja systemu powiadomień wykorzystującego dedykowany serwer SMTP lub pośredniczące konto e-mail. 84. Przedstawienie dostępnych narzędzi monitorowania stanu różnego typu urządzeń, które udostępniają stan poszczególnych parametrów i ustawień poprzez protokół SNMP. 85. Omówienie zasad oraz metod wykonywania aktualizacji oprogramowania serwera NAS w przypadku pojedynczego serwera oraz klastra wysokiej dostępności. 86. Automatyzacja procesu wykonywania kopii zapasowej podstawowej konfiguracji systemu. Objaśnienie co dokładnie zawiera ta kopia, w jaki sposób można ją przywrócić i jakie są ograniczenia z tym związane. 87. Sprzęt i konserwacja. 88. Szczegółowe omówienie specyfikacji sprzętowej oferowanego serwera NAS oraz możliwości jego rozbudowy. 89. Przedstawienie instrukcji wymiany pamięci RAM oraz montowania dodatkowych kart rozszerzeń. 90. Omówienie procesu wymiany podzespołów podczas pracy takich jak dyski HDD. 91. Przedstawienie schematu działania w przypadku wystąpienia problemów z połączeniem do systemu zarządzania serwerem NAS lub w przypadku zatrzymania działania niektórych usług. 92. Symulacja różnych typów awarii, które mogą wystąpić podczas użytkowania serwera i sposobów szybkiego rozwiązywania powstałych problemów. 93. Instruktarz dotyczący bezpiecznego czyszczenia serwera NAS z wymontowaniem niektórych podzespołów. | SPEŁNIA TAK /NIE |

## C WDROŻENIE I SZKOLENIE PRZEŁĄCZNIKÓW

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **Wdrożenie** | * + - 1. Przedmiotem zamówienia jest wdrożenie dwóch zaawansowanych przełączników sieciowych w infrastrukturze Zamawiającego, z kluczowym celem utworzenia stosu (stack) w celu zwiększenia wydajności i niezawodności sieci. Przełączniki mają zostać połączone w stos za pomocą dedykowanych kabli o długości 1 metra, co umożliwi scentralizowane zarządzanie oraz poprawi skalowalność sieci.   2. Zakres prac:  2.1. Dostawa i instalacja sprzętu:   * Dostawa przełączników do lokalizacji wskazanej przez Zamawiającego. * Instalacja fizyczna: Montaż przełączników w istniejących szafach rackowych, uwzględniająca montaż urządzeń, podłączenie do systemu zasilania awaryjnego (UPS) oraz połączenie z istniejącą infrastrukturą sieciową.   2.2. Konfiguracja stosu (stacku):   * Agregacja przełączników w stos: Połączenie obu przełączników za pomocą dedykowanego kabla o długości 1 metra, tworząc pojedynczy, logiczny przełącznik z centralnym punktem zarządzania. * Konfiguracja master/slave: Ustalenie hierarchii przełączników w stosie, z przypisaniem roli urządzenia nadrzędnego (master) oraz podrzędnego (slave). * Synchronizacja konfiguracji: Zastosowanie konfiguracji globalnej, aby ustawienia dotyczące VLAN-ów, routingu oraz polityk bezpieczeństwa były identyczne na wszystkich urządzeniach w stosie.   2.3. Konfiguracja sieciowa:   * Konfiguracja VLAN-ów: Stworzenie i konfiguracja VLAN-ów zgodnie z wymaganiami Zamawiającego, w tym VLAN-ów dedykowanych dla różnych segmentów sieci (np. administracji, serwerów, gości). * Routing między VLAN-ami: Umożliwienie routingu między VLAN-ami w celu zapewnienia bezpiecznej i wydajnej komunikacji między różnymi segmentami sieci. * Implementacja redundancji: Wdrożenie mechanizmów redundancji sieciowej poprzez konfigurację protokołów, które zapewniają nieprzerwane działanie sieci w przypadku awarii jednego z przełączników.   2.4. Testowanie i weryfikacja:   * Testy funkcjonalne: Przeprowadzenie testów mających na celu weryfikację poprawności działania skonfigurowanego stosu, w tym synchronizacji przełączników oraz poprawności funkcjonowania sieci po ich połączeniu. * Testy wydajnościowe: Przeprowadzenie testów przepustowości oraz szybkości przełączania, aby zapewnić optymalne działanie sieci w warunkach produkcyjnych. * Testy awaryjne: Sprawdzenie skuteczności redundancji poprzez symulację awarii jednego z przełączników i weryfikację, czy sieć nadal funkcjonuje bez przerw.   2.5. Szkolenie:   * Szkolenie zespołu IT Zamawiającego w zakresie zarządzania wdrożonym stosem przełączników, obejmujące konfigurację VLAN-ów, zarządzanie stosem oraz podstawową diagnostykę i rozwiązywanie problemów. | SPEŁNIA TAK /NIE |

## D Wdrożenie i SZKOLENIE SYSTEMU NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | **Wdrożenie i szkolenie** | **Etap I. Przygotowanie wdrożenia**  1. Uzgodnienie wymagań technicznych i przygotowanie przez Klienta zasobów niezbędnych do realizacji prac wdrożeniowych  **Etap II: Wdrożenie rozwiązania**  1. Import maszyny wirtualnej na platformę wirtualizacyjną (VMware lub Hyper-V)  2. Konfiguracja parametrów sieciowych i lokalnych interfejsów sieciowych  3. Konfiguracja powiadomień mailowych  4. Konfiguracja integracji z Active Directory  5. Konfiguracja integracji z Windows Management Instrumentation (WMI)  6. Krótki instruktaż dla administratora  7. Podsumowanie wdrożenia - ewentualne pytania  8. Odbiór prac wdrożeniowych  **Etap III. Szkolenie: konfiguracja i administrowanie rozwiązaniem NAC (4 godz. zdalnie)**  Agenda:  1. NAC - sposób działania i wykorzystanie w infrastrukturze IT  2. Interfejs administratora  3. Konfiguracja sieciowa rozwiązania  4. Monitorowanie sieci i blokowanie dostępu (Device Manager, Network Map)  5. Ochrona przed spoofingiem (fingerprinting)  6. Powiadomienia mailowe  7. Automatyczna klasyfikacja urządzeń (Device Profiler, Auto Trust)  8. Zarządzanie dostępem (Roles & Access, ACLs)  9. Integracja z innymi systemami (AD, AV, WMI, Syslog & Email Orchestration)  10. Rejestrowanie urządzeń prywatnych i dostęp gości (Captive Portal)  11. Raporty (Device Manager Reports, Network Inventory)  12. Aktualizacja firmware  Etap IV. Konsultacje powdrożeniowe (4 godz. zdalnie)  1. Przegląd działania rozwiązania 1-3 miesiące od zakończenia wdrożenia  2. Odpowiedzi na pytania związane z eksploatacją rozwiązania NAC  Wymaga się, aby dostawca przedstawił:  - oświadczenie Producenta/lub autoryzowanego Dystrybutora, o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia należy załączyć do oferty  - osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie , należy załączyć do oferty | SPEŁNIA TAK /NIE |

## E Wdrożenie i SZKOLENIE SYSTEMU ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP)

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **1** | **Wdrożenie i konfiguracja** | 1. Przedmiot zamówienia  Przedmiotem zamówienia jest wdrożenie systemu klasy DLP (Data Loss Prevention) na infrastrukturze serwerowej Zamawiającego. Wdrożenie obejmuje konfigurację serwera bazodanowego, instalację i konfigurację oprogramowania na serwerze wirtualnym oraz przeszkolenie personelu Zamawiającego.  2. Zakres zamówienia  Zakres zamówienia obejmuje następujące elementy:   1. Konfiguracja serwera bazodanowego:    * Przygotowanie serwera bazodanowego: Ustawienie środowiska bazodanowego zgodnie z wymaganiami systemu DLP. Konfiguracja instancji bazy danych obejmująca odpowiednie parametry wydajnościowe i bezpieczeństwa.    * Integracja z systemem DLP: Połączenie bazy danych z oprogramowaniem DLP, zapewniając jej optymalną współpracę i wydajność. 2. Instalacja i konfiguracja na serwerze wirtualnym:    * Przygotowanie środowiska serwera wirtualnego: Instalacja systemu operacyjnego oraz wszystkich niezbędnych komponentów na serwerze wirtualnym dostarczonym przez Zamawiającego.    * Instalacja oprogramowania DLP: Zainstalowanie systemu DLP na serwerze wirtualnym, zgodnie z wymaganiami technicznymi dostawcy oprogramowania.    * Konfiguracja systemu: Ustawienie reguł bezpieczeństwa, polityk monitorowania i ochrony danych zgodnie z potrzebami Zamawiającego. Konfiguracja modułów monitorowania, raportowania oraz alertów w systemie DLP. 3. Integracja z infrastrukturą sieciową:    * Połączenie z istniejącymi systemami: Integracja systemu DLP z infrastrukturą sieciową Zamawiającego, w tym z serwerami plików, pocztą e-mail oraz innymi krytycznymi usługami.    * Testowanie połączeń i funkcjonalności: Weryfikacja poprawności działania systemu DLP w rzeczywistym środowisku produkcyjnym. Testowanie reguł ochrony oraz raportowania w celu zapewnienia zgodności z założonymi wymaganiami. 4. Szkolenie:    * Szkolenie zespołu IT Zamawiającego: Przeprowadzenie szkolenia dla zespołu odpowiedzialnego za zarządzanie i obsługę systemu DLP. Szkolenie obejmuje:      + Podstawy konfiguracji i zarządzania systemem DLP.      + Zarządzanie incydentami i alertami.      + Tworzenie i modyfikowanie polityk bezpieczeństwa.      + Monitorowanie i raportowanie działań w systemie DLP.      + Szkolenie minimum 6 godzin    * Dokumentacja: Dostarczenie szczegółowej dokumentacji dotyczącej wdrożonego systemu oraz | SPEŁNIA TAK /NIE |

## F WDROŻENIE I SZKOLENIE SYSTEMÓW SYSTEM DETEKCJI I REAKCJI NA ZDARZENIA W KOŃCOWYCH PUNKACH – EDR

## SYSTEMU ZARZĄDZANIA INFORMACJAMI I ZDARZENIAMI BEZPIECZEŃSTWA INFORMATYCZNEGO - SIEM

## OPROGRAMOWANIA ANTYWIRUSOWEGO DEDYKOWANE DO SERWERÓW

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| **1** | **Wdrożenie i szkolenie** | 1. Przedmiot zamówienia  Przedmiotem zamówienia jest wdrożenie oraz konfiguracja zintegrowanego systemu zabezpieczeń obejmującego zaawansowane narzędzia do wykrywania zagrożeń, zarządzania podatnościami oraz monitorowania aktywności sieciowej. System ma zostać wdrożony na infrastrukturze Zamawiającego, z pełną konfiguracją oraz przeszkoleniem personelu.  2. Zakres zamówienia  Zakres zamówienia obejmuje następujące elementy:   1. Instalacja i konfiguracja narzędzia do wykrywania zagrożeń (XDR):    * Przygotowanie środowiska serwerowego: Instalacja oprogramowania na dedykowanych serwerach lub wirtualnych maszynach, zapewniająca optymalną wydajność i skalowalność systemu.    * Konfiguracja agentów: Instalacja agentów monitorujących na stacjach roboczych, serwerach oraz innych urządzeniach sieciowych w infrastrukturze Zamawiającego.    * Ustawienie reguł wykrywania: Skonfigurowanie reguł wykrywania zagrożeń, monitorowania incydentów oraz reagowania na wykryte zagrożenia zgodnie z politykami bezpieczeństwa Zamawiającego.    * Integracja z istniejącymi systemami: Połączenie systemu z narzędziami zarządzania logami (SIEM) oraz innymi elementami infrastruktury IT w celu zapewnienia kompleksowej ochrony. 2. Instalacja i konfiguracja narzędzia do zarządzania podatnościami:    * Skany początkowe: Przeprowadzenie początkowych skanów podatności na wszystkich krytycznych zasobach IT Zamawiającego.    * Konfiguracja harmonogramów skanowania: Ustalenie regularnych harmonogramów skanowania, które będą automatycznie identyfikować nowe podatności oraz oceniać ryzyko związane z nimi.    * Raportowanie: Konfiguracja systemu raportowania, który będzie dostarczał regularne raporty na temat stanu zabezpieczeń oraz rekomendacje dotyczące działań naprawczych.    * Integracja z narzędziem XDR: Skonfigurowanie automatycznego przekazywania wyników skanowania do systemu wykrywania zagrożeń, co umożliwi bardziej dynamiczne reagowanie na wykryte podatności. 3. Instalacja i konfiguracja narzędzia do monitorowania aktywności sieciowej:    * Monitorowanie w czasie rzeczywistym: Ustawienie monitoringu sieciowego w celu wykrywania nietypowych zachowań i potencjalnych zagrożeń w czasie rzeczywistym.    * Analiza ruchu sieciowego: Skonfigurowanie analizy ruchu sieciowego, z naciskiem na wykrywanie anomalii, które mogą wskazywać na próby włamań lub inne formy cyberataków.    * Zarządzanie alertami: Konfiguracja systemu alertów, który powiadomi odpowiednie osoby lub zespoły w przypadku wykrycia podejrzanych działań. 4. Szkolenie personelu:    * Szkolenie z obsługi systemu: Przeprowadzenie szkolenia dla zespołu IT Zamawiającego, obejmującego zarządzanie każdym z wdrożonych narzędzi, w tym:      + Monitorowanie i zarządzanie wykrytymi zagrożeniami.      + Tworzenie i modyfikowanie polityk bezpieczeństwa.      + Przeprowadzanie skanów podatności oraz interpretacja wyników.      + Zarządzanie i reagowanie na alerty związane z aktywnością sieciową.      + Szkolenie minimum 10 godzin 5. **Dla zapewnienia wysokiego poziomu usług podmiot wdrażający rozwiązanie musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem.** | SPEŁNIA TAK /NIE |

**Niespełnienie któregokolwiek z wymaganych parametrów oraz wymagań co do nich wartości minimalnych spowoduje odrzucenie oferty bez dalszej jej oceny jako oferta niezgodna z warunkami zamówienia.**