Załącznik nr 1 do SWZ

Spis treści

[1 Część I 2](#_Toc191913605)

[1.1 Serwer z oprogramowaniem 2 Szt. 2](#_Toc191913606)

[1.2 Macierz dyskowa 1 szt. 12](#_Toc191913607)

[1.3 Serwer do Backupu 1 szt. 20](#_Toc191913608)

[1.4 Serwerowy system operacyjny 3 szt. 31](#_Toc191913609)

[1.5 Licencje dostępowe CAL 250 szt. 32](#_Toc191913610)

[1.6 System zarządzania bazą danych 2 szt. 32](#_Toc191913611)

[1.7 Instalacja, konfiguracja, wdrożenie, utrzymanie części I 33](#_Toc191913612)

[2 Część II 34](#_Toc191913613)

[2.1 Firewall 2 szt. 34](#_Toc191913614)

[2.2 Centralny system logów 1 szt. 42](#_Toc191913615)

[2.3 Przełącznik sieci LAN CORE 2 szt. 45](#_Toc191913616)

[2.4 Przełącznik sieci LAN IDF 2 szt. 48](#_Toc191913617)

[2.5 Access Point 5 szt. 52](#_Toc191913618)

[2.6 Instalacja, konfiguracja, wdrożenie, utrzymanie części II 53](#_Toc191913619)

[3 Część III 53](#_Toc191913620)

[3.1 System EDR-XDR 54](#_Toc191913621)

[3.2 Oprogramowanie do zarządzania siecią IT – aktualizacja licencji do 300 szt. 60](#_Toc191913622)

[3.3 Instalacja, konfiguracja, wdrożenie, utrzymanie części III 69](#_Toc191913623)

[4 Część IV 69](#_Toc191913624)

[4.1 System SIEM-SOAR 70](#_Toc191913625)

[4.2 Instalacja, konfiguracja, wdrożenie, utrzymanie części IV 91](#_Toc191913626)

WYMAGANIA MINIMALNE ZAOFEROWANEGO ASORTYMENTU:

# Część I

## Serwer z oprogramowaniem 2 Szt.

2 sztuki:

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5” * Obudowa z możliwością wyposażenia 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 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. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania dwóch procesorów. * Możliwość obsługi procesorów 128 rdzeniowych * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do min. 6TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Zainstalowane dwa procesory, min. 16-rdzeniowe, min. 3.0GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 353 w teście SPECrate2017\_int\_base w konfiguracji dwu procesorowej, dostępnym na stronie www.spec.org. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 5600MT/s, |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, musi posiadać możliwość konfiguracji poziomów RAID: 0, 1, 10 |
| **Dyski twarde** | * Zainstalowane:   + 1x dysk SAS o pojemności min. 600GB Hot-Plug. * Możliwość zainstalowania, w dedykowanym slocie, dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Minimum osiem slotów PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT * Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 |
| **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 obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1000W klasy Titanium |
| **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 |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * 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). |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiada 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 automatycznej rejestracji 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) |
| **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. |
| **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 seryjnym     - 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 aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji 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 |
| **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 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 musi posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego lub na stronie internetowej producenta sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **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. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * 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 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 musi posiadać 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 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 musi posiadać autoryzacje producenta urządzeń. |

## Macierz dyskowa 1 szt.

| **Cecha** | **Opis Wymagań** |
| --- | --- |
| **Obudowa** | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 8U. |
| **Kontrolery dyskowe** | Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Kontrolery nie mogą pracować w trybie active-passive. Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych. |
| **CPU** | Wymagany min 1 procesor per kontroler min 8 rdzeni każdy. Macierz musi dostarczać sumarycznie min 16 rdzeni. |
| **Wymagana przestrzeń** | Fizyczna przestrzeń dyskowa zbudowana za pomocą dysków SSD SAS oraz HDD NL SAS. Wymagana przestrzeń RAW na dyskach SSD SAS musi wynosić min 1.92 TB. Przestrzeń RAW na dyskach NL SAS musi wynosić min 40 TB RAW.  Wymagana możliwość rozbudowy przestrzeni użytkowej do 500 TB poprzez instalację dysków oraz półek dyskowych. Rozbudowa musi być wykonywana w sposób online, bez przerwy w dostępie do danych. |
| **Zabezpieczenia dyskami SPARE** | Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
| **Pamięć Cache** | Co najmniej 64GB pamięci cache na całą macierz (dwa kontrolery). Pamięć cache do zapisu musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |
| **Dostępne porty front-end** | Razem kontrolery muszą udostępnić do hostów minimum 4 porty 1Gb Eth oraz 4 porty 10Gb Eth SFP+ (wymagane wkładki optyczne). Wymagana możliwość rozbudowy o dodatkowe 8 portów 25Gb Eth SFP+ bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu. |
| **Obsługiwane protokoły** | Wymagane wsparcie dla FC, iSCSI, NFS, CIFS. Nie dopuszcza się wsparcia dla protokołów plikowych poprzez zastosowanie dodatkowego gateway’a / główki NAS. Protokoły NFS i CIFS muszą być natywnie wspierane przez oferowaną macierz. |
| **Obsługiwane typy zabezpieczenia RAID** | Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych. |
| **Prezentacja dysków logicznych** | Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Wymagane dostarczenie w/w funkcjonalność na zainstalowana przestrzeń dyskową.  Max liczba wolumenów blokowych (LUN) obsługiwanych przez macierz nie może być mniejsza niż 2000.  Max liczba file system’ów (NAS) obsługiwanych przez macierz nie może być mniejsza niż 500. |
| **Zarządzanie** | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS.  Wymagane jest stałe monitorowanie wydajności obiektów takich jak:  - cała macierz  - kontrolery  - porty front-end  - dyski  - LUNy  - file systemy  - hosty  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - średnie użycie CPU (w %)  Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.  Centralne zarządzanie   * Macierz dyskowa powinna być wyposażona w moduł zarządzania, który umożliwia kontrolę wszystkich zasobów z poziomu jednego interfejsu graficznego (GUI) lub interfejsu wiersza poleceń (CLI). * Moduł zarządzania pozwala na konfigurację, monitorowanie oraz optymalizację pracy macierzy w czasie rzeczywistym.   Monitorowanie systemu   * Moduł zarządzania oferuje stałe monitorowanie stanu macierzy, kontrolerów, dysków oraz portów sieciowych. * Możliwość monitorowania kluczowych wskaźników wydajności, takich jak IOPS (operacje wejścia/wyjścia na sekundę), przepustowość, czas odpowiedzi (latency) oraz średnie użycie procesora. * Zintegrowane zarządzanie alarmami i powiadomieniami o zdarzeniach krytycznych.   Interfejs zarządzania   * Macierz dyskowa musi posiadać dedykowany port zarządzania (Ethernet 1 GbE), który umożliwia bezpieczny dostęp do modułu zarządzania. * Możliwość zdalnego zarządzania poprzez przeglądarkę internetową (GUI) lub interfejs wiersza poleceń (CLI).   Obsługa standardowych protokołów zarządzania, takich jak SNMP, Redfish API, oraz możliwość integracji z systemami monitorowania zewnętrznego. |
| **Kopie wewnątrz macierzy** | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) wolumenów blokowych (LUN) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Wymagana jest możliwość utworzenia harmonogramu snapshotów. Macierz musi umożliwiać utworzenie min 800 snapshotów wolumenów blokowych (LUN). Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware.  Wymagana również obsługa snapshotów file systemów.  Dostarczenie powyższych funkcjonalności jest wymagane na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.  Wymagana możliwość tworzenia na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagane możliwość resynchronizacji klona z wolumenem źródłowym (LUN). |
| **Kontrola zasobów plikowych (NAS)** | Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.  Wymagana możliwość konfiguracji uprawnień użytkowników typu read-only oraz read-write per wystawiony udział NAS.  Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania. |
| **Ochrona plików** | Wymagana możliwość skonfigurowania funkcjonalności typu WORM, która blokuje pliki przed usunięciem lub modyfikacją. Zabezpieczone pliki mają pozostać tylko do odczytu przez skonfigurowany okres czasu. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania. |
| **Tiering** | Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych bez konieczności rekonfiguracji po stronie serwerów korzystających z wolumenów logicznych. Dostarczenie licencji na tą funkcjonalność jest wymagane. |
| **Replikacja danych** | Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybach synchroniczna oraz asynchroniczna przy wykorzystaniu portów FC lub IP. Dostarczenie licencji dla tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| **Klaster macierzowy** | Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych przy wykorzystaniu portów FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną.  Dostarczenie licencji dla tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| **Priorytety zadań** | Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania. |
| **Funkcjonalności BIOS i firmware** | Oferowana macierz dyskowa musi być wyposażona w zaawansowany system firmware'u, który zapewnia pełną kontrolę nad sprzętem oraz podstawowe funkcje zarządzania i diagnostyki. Firmware musi spełniać następujące wymagania:  1. Inicjalizacja sprzętu  Firmware macierzy musi umożliwiać pełną inicjalizację wszystkich kluczowych komponentów, takich jak kontrolery, pamięć cache, moduły dyskowe oraz porty sieciowe.  System musi sprawdzać stan komponentów podczas rozruchu, identyfikując ewentualne problemy i sygnalizując je za pomocą wskaźników oraz alertów w interfejsie zarządzania.  2. Konfiguracja kontrolerów  Firmware musi umożliwiać konfigurację parametrów pracy kontrolerów macierzy, w tym ustawień RAID, alokacji pamięci cache oraz konfiguracji portów front-end i back-end.  Wymagana jest funkcja zarządzania zasilaniem, która pozwala na dostosowanie parametrów pracy macierzy w celu optymalizacji zużycia energii.  3. Zarządzanie pamięcią cache  Firmware macierzy musi zapewniać dynamiczne zarządzanie pamięcią cache, umożliwiając optymalne wykorzystanie jej zasobów pomiędzy operacjami odczytu i zapisu.  Wymagana jest funkcja zabezpieczenia danych w pamięci cache, obejmująca automatyczne zapisanie zawartości cache na pamięć nieulotną (NVRAM) w przypadku awarii zasilania.  4. Bezpieczeństwo rozruchu  Firmware musi wspierać funkcję Secure Boot, która zapobiega uruchamianiu nieautoryzowanego oprogramowania. Oprogramowanie musi sprawdzać integralność systemu przed jego uruchomieniem, aby zabezpieczyć macierz przed potencjalnym złośliwym kodem.  Wymagane jest wsparcie dla zarządzania certyfikatami oraz integracji z systemami uwierzytelniania.  5. Monitorowanie stanu systemu  Firmware musi stale monitorować stan kluczowych komponentów macierzy, takich jak procesory kontrolerów, pamięć RAM, dyski oraz porty sieciowe.  Wymagana jest funkcjonalność raportowania stanu systemu do interfejsu zarządzania, z możliwością przeglądania historii zdarzeń oraz alertów w czasie rzeczywistym.  6. Aktualizacje firmware'u bez przerywania pracy  Firmware musi umożliwiać aktualizację oprogramowania bez przerywania pracy macierzy oraz bez konieczności wyłączania dostępu do danych. Aktualizacje muszą być możliwe do wykonania online, z poziomu interfejsu zarządzania.  Wymagane jest wsparcie dla automatycznych aktualizacji oraz powiadomień o dostępnych poprawkach bezpieczeństwa.  7. Diagnostyka i raportowanie  Firmware musi oferować funkcje diagnostyczne, które umożliwiają przeprowadzanie testów sprzętowych oraz zbieranie logów systemowych.  Wymagana jest możliwość generowania raportów diagnostycznych oraz eksportowania logów do analizy w celu szybkiego identyfikowania problemów i podejmowania działań naprawczych.  System musi umożliwiać dostęp do logów oraz wyników testów diagnostycznych z poziomu interfejsu graficznego (GUI) oraz wiersza poleceń (CLI). |
| **Zaawansowany system diagnostyczny** | Oferowana macierz dyskowa musi być wyposażona w zaawansowany system diagnostyczny, który zapewnia kompleksowe monitorowanie stanu systemu, szybkie wykrywanie problemów oraz proaktywne działania serwisowe. System diagnostyczny musi spełniać następujące wymagania:  1. Stałe monitorowanie stanu komponentów   * System diagnostyczny musi umożliwiać ciągłe monitorowanie stanu wszystkich kluczowych komponentów macierzy, w tym:   + Procesorów kontrolerów.   + Pamięci RAM i pamięci cache.   + Dysków SSD i HDD.   + Portów sieciowych front-end (Ethernet, Fibre Channel) oraz portów back-end (SAS). * System musi monitorować parametry takie jak temperatura, napięcie, prędkość wentylatorów oraz stan zdrowia dysków, sygnalizując wszelkie nieprawidłowości w czasie rzeczywistym.   2. Diagnostyka dysków twardych   * Oprogramowanie musi oferować funkcję monitorowania stanu zdrowia dysków, w tym wykrywanie błędów S.M.A.R.T. oraz analizę żywotności dysków SSD. * System musi umożliwiać wczesne ostrzeganie przed awarią dysku (Predictive Failure Analysis), co pozwala na planową wymianę dysku przed jego uszkodzeniem. * Diagnostyka dysków musi obejmować możliwość uruchamiania testów diagnostycznych, zarówno ręcznie przez administratora, jak i automatycznie w ramach rutynowej konserwacji.   3. System raportowania i powiadomień   * System diagnostyczny musi generować automatyczne raporty o stanie systemu, zawierające informacje o błędach, ostrzeżeniach oraz potencjalnych problemach. * Wymagana jest funkcjonalność automatycznego powiadamiania administratorów o krytycznych zdarzeniach za pomocą e-maila, protokołów SNMP lub innych narzędzi monitorujących. * W przypadku wykrycia problemu, system musi automatycznie zapisywać logi zdarzeń oraz dane diagnostyczne, które będą dostępne do analizy.   4. Automatyczne testy diagnostyczne   * System musi przeprowadzać automatyczne testy diagnostyczne sprzętu podczas rozruchu oraz w trakcie normalnej pracy, aby wykrywać problemy bez przerywania działania macierzy. * W przypadku wykrycia nieprawidłowości, system musi być w stanie automatycznie podjąć działania naprawcze, takie jak przełączenie ścieżki dostępu na zdrowy kontroler lub wyłączenie wadliwego dysku z użytku.   5. Analiza wydajności i optymalizacja   * System diagnostyczny musi monitorować wydajność macierzy, analizując kluczowe wskaźniki, takie jak:   + Liczba operacji wejścia/wyjścia na sekundę (IOPS).   + Przepustowość (KB/s lub MB/s).   + Opóźnienia (latency).   + Wykorzystanie zasobów procesora (CPU usage). * System musi oferować funkcje analizy wydajności oraz rekomendacje dotyczące optymalizacji pracy macierzy, identyfikując potencjalne wąskie gardła.   6. Proaktywne wsparcie serwisowe   * System diagnostyczny musi być zintegrowany z narzędziami zdalnego wsparcia, umożliwiając przesyłanie danych diagnostycznych do centrum serwisowego producenta. * Wsparcie musi obejmować proaktywne monitorowanie stanu systemu oraz predykcyjne utrzymanie (predictive maintenance), co pozwala na identyfikację problemów zanim wpłyną one na działanie systemu.   7. Zarządzanie logami i historia zdarzeń   * System musi umożliwiać zapis i przeglądanie logów zdarzeń oraz historii diagnostyki sprzętu, co pozwala na szczegółową analizę problemów i śledzenie zmian stanu systemu. * Administrator musi mieć możliwość eksportowania logów i raportów diagnostycznych do dalszej analizy lub przesłania ich do centrum serwisowego w celu wsparcia technicznego.   8. Integracja z narzędziami zarządzania  System diagnostyczny musi obsługiwać standardowe protokoły zarządzania, takie jak SNMP, Redfish API, co umożliwia integrację z zewnętrznymi systemami monitorowania i zarządzania. |
| **Oprogramowanie do zarządzania macierzą** – w formularzu należy podać pełną nazwę oferowanego oprogramowania | Oferowana macierz dyskowa musi być wyposażona w dedykowane oprogramowanie zarządzające, które zapewnia kompleksowe zarządzanie, monitorowanie oraz optymalizację pracy systemu. Oprogramowanie powinno obejmować następujące funkcjonalności:  1. Intuicyjny interfejs graficzny (GUI)   * Oprogramowanie do zarządzania macierzą musi zapewniać:   + Przyjazny interfejs graficzny: Umożliwiający łatwą konfigurację, zarządzanie oraz monitorowanie wszystkich zasobów macierzy dyskowej.   + Monitorowanie wydajności w czasie rzeczywistym: System musi prezentować dane dotyczące wydajności macierzy, takie jak operacje wejścia/wyjścia (IOPS), przepustowość, opóźnienia oraz wykorzystanie zasobów, w formie wykresów i raportów.   + Zarządzanie alarmami: Oprogramowanie musi obsługiwać zarządzanie alarmami, w tym powiadamianie o zdarzeniach krytycznych i ostrzeżeniach oraz możliwość konfiguracji polityk alarmowych.   + Zarządzanie użytkownikami: System musi umożliwiać tworzenie różnych ról i uprawnień dla użytkowników, zapewniając bezpieczny dostęp do funkcji administracyjnych.   2. Interfejs wiersza poleceń (CLI)   * Oprogramowanie musi oferować:   + Zaawansowane zarządzanie przez wiersz poleceń: Interfejs wiersza poleceń musi umożliwiać wykonywanie zaawansowanych operacji konfiguracyjnych oraz diagnostycznych.   + Wsparcie dla automatyzacji: System musi obsługiwać tworzenie skryptów automatyzujących rutynowe zadania administracyjne, co zwiększa efektywność zarządzania.   3. Narzędzia serwisowe i konserwacyjne   * Oprogramowanie musi zawierać zestaw narzędzi wspierających rutynową konserwację, w tym:   + Aktualizacje i instalacja poprawek: Możliwość przeprowadzania aktualizacji oprogramowania macierzy oraz instalacji poprawek bez przerywania dostępu do danych.   + Automatyczne inspekcje: Oprogramowanie musi umożliwiać automatyczne inspekcje stanu macierzy, identyfikując potencjalne problemy przed ich eskalacją.   + Narzędzia do diagnostyki: System musi oferować narzędzia do szybkiej diagnostyki i rozwiązywania problemów, co ułatwia konserwację i naprawę sprzętu.   4. Zdalne monitorowanie i wsparcie   * Oprogramowanie musi zapewniać funkcje zdalnego monitorowania oraz wsparcia technicznego przez producenta, w tym:   + Zdalny dostęp do systemu: Możliwość zdalnego monitorowania stanu macierzy oraz zdalnego przesyłania plików diagnostycznych do serwisu, co ułatwia wsparcie techniczne.   + Powiadomienia o alarmach: System musi automatycznie generować powiadomienia o błędach i ostrzeżeniach, z możliwością przesyłania informacji do administratora poprzez e-mail lub protokół zarządzania (SNMP).   + Integracja z platformą analityczną: Oprogramowanie musi umożliwiać analizę danych operacyjnych oraz wspierać funkcje predykcyjnego utrzymania, co pozwala na proaktywne działania serwisowe.   5. Wymagania dodatkowe   * Oprogramowanie musi być dostarczone przez producenta macierzy i zapewniać pełną kompatybilność z oferowanym sprzętem. * Oprogramowanie musi być dostępne w języku polskim lub angielskim.   Producent musi zapewniać wsparcie techniczne oraz regularne aktualizacje oprogramowania przez okres trwania gwarancji. |
| **Wspierane systemy operacyjne** | Wsparcie, dla co najmniej Microsoft Server Windows 2019/2022, VMware 7.x/8.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x |
| **Gwarancja i serwis** | Wymagane uaktualnianie firmware kontrolerów macierzy bez przerywania dostępu do danych.  Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.  Macierz musi umożliwiać zdalne zarządzanie.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego.  Wymagana gwarancja na 3 lata w trybie 24/7 z naprawą realizowaną w miejscu instalacji. Uszkodzone dyski pozostają u Zamawiającego.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także oferowanego oprogramowania.  Wymagane dołączenie do oferty oświadczenia producenta 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 autoryzacje producenta urządzeń. |

## Serwer do Backupu 1 szt.

|  |  |
| --- | --- |
| **Obudowa** | * Obudowa Rack o wysokości 2U * 12 wnęk na dyski 3.5” * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * 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. |
| **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. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **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. |
| **RAM** | * 512GB DDR5 RDIMM 5600MT/s, |
| **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 |
| **Dyski twarde** | * Zainstalowane:   + 6x dysk SSD SATA o pojemności min. 960GB, Hot-Plug   + 6x dysk SAS o pojemności min. 12TB, Hot-Plug * Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Sześć slotów PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **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 obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | * Redundantne, Hot-Plug |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1000W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * 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). |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego musi posiadać 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 automatycznej rejestracji 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) |
| **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. |
| **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 musi posiadać 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 aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji 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 |
| **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 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 musi posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego lub na stronie internetowej producenta sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **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. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * 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 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 musi posiadać 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 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 musi posiadać autoryzacje producenta urządzeń. |

## Serwerowy system operacyjny 3 szt.

Serwerowy System operacyjny

* 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.

## Licencje dostępowe CAL 250 szt.

**Licencje dostępowe CAL – 250 szt. o parametrach nie gorszych lub równoważnych.**

Zamawiający wymaga licencji obejmującej poniższy zakres:

* licencje dożywotnie umożliwiające dostęp 250 użytkownikom do środowiska domenowego opartego o Active Directory Microsoft Windows.
* licencje w najnowszej możliwej wersji.

## System zarządzania bazą danych 1 kpl.

Oprogramowanie serwerowe w wersji Standard, pozwalającego na zarządzanie i przechowywanie danych w relacyjnej bazie danych, zapewniającego funkcjonalności niezbędne do pracy w środowisku biznesowym i analitycznym. Oprogramowanie ma być dostarczone w formie licencji na dwa rdzenie (Core). Zamówienie obejmuje łącznie 2 licencje, każda obejmująca dwa rdzenie.

**Minimalne wymagania techniczne oprogramowania**

1. Rodzaj oprogramowania:
   * Oprogramowanie serwerowe przeznaczone do zarządzania relacyjnymi bazami danych w środowiskach wielowątkowych i wielordzeniowych.
2. Wymagania dotyczące funkcjonalności:
   * Obsługa zaawansowanych zapytań w języku SQL.
   * Możliwość korzystania z mechanizmów replikacji danych.
   * Zintegrowane narzędzia analityczne i raportowania.
   * Mechanizmy automatycznego zabezpieczania danych (backup, odzyskiwanie).
   * Obsługa szyfrowania danych w czasie rzeczywistym.
   * Możliwość uruchamiania aplikacji w środowisku chmurowym i lokalnym.
3. Wydajność i kompatybilność:
   * Obsługa co najmniej 2 rdzeni procesorowych na jedną licencję.
   * Wsparcie dla współpracy z najnowszymi wersjami systemów operacyjnych klasy serwerowej.
   * Zgodność z wymaganiami architektury x64.
   * Wsparcie/obsługa używanych u Zamawiającego programów „EZD Proton” i „Sprawny Urząd”.
4. Wersja licencji:
   * Licencja wieczysta (tzw. perpetual).
   * Licencja nowa, nigdy nie aktywowana, pochodząca z oficjalnego kanału dystrybucji producenta.
   * Licencja pozwala na przeniesienie / reinstalację na inne urządzenie.
   * Zamawiający nie wymaga aktywacji w modelu Software Assurance, nie wymaga także wpisu w ramach portalu MPSA / Tenant

**Wymagania dotyczące dostawy**

1. Licencje mają być dostarczone w formie elektronicznej (np. licencje elektroniczne) lub w wersji fizycznej (np. nośnik instalacyjny wraz z kluczem licencyjnym).
2. Dostarczone licencje muszą być oryginalne i pochodzić od autoryzowanego dystrybutora.
3. Wykonawca dostarczy wszystkie niezbędne materiały umożliwiające instalację i aktywację oprogramowania, w tym:
   * Dokumentację użytkownika.
   * Warunki licencyjne oraz dowód legalności oprogramowania.
   * Odnośnik do pobrania plików instalacyjnych (strona producenta)

## Instalacja, konfiguracja, wdrożenie, utrzymanie części I

1. Opracowanie z Zamawiającym procedury migracji istniejącej infrastruktury serwerowej na nowe serwery i systemy serwerowe

W ramach tego zadania wykonawca będzie odpowiedzialny za opracowanie szczegółowej procedury migracji, która obejmie:

Migracja Active Directory: Dodanie nowego kontrolera domeny (DC) do istniejącej infrastruktury AD, wygaszenie starego kontrolera oraz jego ponowne postawienie. Proces migracji będzie realizowany przy użyciu skryptów, co zapewni automatyzację i minimalizację błędów.

Migracja systemów plików (FS) i integracja z Active Directory w celu zachowania spójności i integralności danych.

Migracja serwerów aplikacji: Połączenie z nową bazą danych SQL Server, migracja danych oraz konfiguracja serwerów aplikacji.

Migracja systemów OpenSource: Przeniesienie środowisk opartych na Debianie i Ubuntu na nową platformę sprzętową, zapewniając kompatybilność i wydajność nowych serwerów.

2. Instalacja i wstępna konfiguracja 2 systemów serwerowych do współpracy z macierzą dyskową

W ramach tego zadania wykonawca zainstaluje oraz przeprowadzi wstępną konfigurację dwóch serwerów Windows Server, które będą współpracować z macierzą dyskową zgodnie z opracowaną procedurą migracji. Celem jest zapewnienie pełnej integracji serwerów z systemem przechowywania danych, uwzględniając odpowiednią konfigurację RAID, dostępności i redundancji.

3. Instalacja i konfiguracja systemu Windows Server na Serwerze do backupu

Wykonawca zainstaluje i skonfiguruje system Windows Server na dedykowanym serwerze, który będzie pełnił funkcję backupową. Zostaną przeprowadzone testy w celu zapewnienia prawidłowego działania mechanizmów tworzenia kopii zapasowych i ich odzyskiwania.

4. Instalacja i konfiguracja serwera MS SQL w środowisku produkcyjnym

Wykonawca zainstaluje oraz skonfiguruje serwer MS SQL na serwerze produkcyjnym, zgodnie z procedurą migracji. Procedura instalacji obejmie:

Instalację serwera SQL i konfigurację środowiska produkcyjnego,

Migrację danych do nowej bazy SQL Server,

Opracowanie dokumentacji opisującej procedurę instalacji wraz z zapisanymi hasłami,

Dokumentacja stanie się własnością Zamawiającego i będzie podlegała prawom majątkowym.

5. Wsparcie Zamawiającego w utrzymaniu serwerów

Wsparcie w utrzymaniu serwerów przez okres obowiązywania umowy może obejmować:

Zarządzanie kopiami zapasowymi i odzyskiwaniem danych: Zapewnienie bieżącego wsparcia w zarządzaniu kopiami zapasowymi oraz procedurami odzyskiwania danych w przypadku awarii.

Wykonywanie poprawek i aktualizacji oprogramowania: Regularne aktualizacje oprogramowania systemowego, aplikacji serwerowych i baz danych w celu zapewnienia ich bezpieczeństwa i stabilności.

Usuwanie awarii i wsparcie w diagnostyce: Pomoc w rozwiązywaniu problemów związanych z infrastrukturą serwerową, przeprowadzanie diagnostyki oraz wdrażanie rozwiązań naprawczych.

# Część II

## Firewall 2 szt.

**Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musie mieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

**Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

**Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

**Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

**Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

**Testy wydajnościowe oraz funkcjonalne**

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

**Rozszerzone wsparcie serwisowe**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

**Gwarancja oraz wsparcie**

1. System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer musi posiadać certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

## Centralny system logów 1 szt.

**Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

**Interfejsy, Dysk, Zasilanie:**

1. System musi dysponować co najmniej:

* 2 portami Gigabit Ethernet RJ-45.

1. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.
2. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 25 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 500 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

**Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

**Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

**Serwisy i licencje**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Rozszerzone wsparcie serwisowe**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

**Opisy do wymagań ogólnych**

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer musi posiadać certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent musi posiadać autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

## Przełącznik sieci LAN CORE 2 szt.

|  |  |
| --- | --- |
| **Przełącznik sieciowy 24 portów** | 1. Przełącznik musi posiadać minimum 12 portów RJ45 o minimalnej prędkości 10 Gb/s. 2. Przełącznik musi posiadać minimum 12 portów SFP+ o prędkości minimum 10 Gb/s. 3. Przełącznik musi posiadać minimum 1 port RJ45 o minimalnej prędkości 1 Gb/s przeznaczony do zarządzania typu OOB. 4. Przełącznik musi posiadać porty konsolowe typu RJ-45 oraz USB typu C. 5. Przełącznik musi umożliwiać montaż w standardowej szafie rack 19”. 6. Przepustowość przełącznika nie może być mniejsza niż 480 Gb/s. 7. Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 357,12 Mp/s, (pakiety wielkości 64 bajtów). 8. Przełącznik musi pozwalać na Stacking sprzętowy. 9. Wielkość bufora pakietów nie może być mniejsza niż 8 MB. 10. Przełącznik musi obsługiwać technologię drzewa rozpinającego w przynajmniej w wersji: 11. STP (IEEE 802.1d) 12. RSTP (IEEE 802. 1w) 13. MSTP (IEEE 802. 1s) 14. Przełącznik musi pozwalać na zabezpieczenie protokołu drzewa rozpinającego za pomocą: 15. BPDU 16. STP Root Guard 17. STP loopback guard 18. Przełącznik musi wspierać agregację portów przynajmniej w oparciu o protokół 802.3ad 19. Przełącznik musi posiadać wsparcie dla technologii 802.1Q. 20. Przełącznik musi posiadać wsparcie przynajmniej dla takich protokołów jak: 21. MAC VLAN 22. IP VLAN 23. Management VLAN 24. QinQ 25. Voice VLAN 26. VLANy prywatne 27. PVE 28. Multicast TV VLAN 29. Dynamiczne przydzielanie VLAN’ów w ramach uwierzytelniania oraz autoryzacji 802.1X/RADIUS 30. Przełącznik musi wspierać wykrywanie uszkodzeń warstwy pierwszej, które mogą powodować pętle. 31. Przełącznik musi zapewniać obsługę przekazywania ruchu DHCP pomiędzy VLAN’ami wraz z obsługa opcji 82. 32. Przełącznik musi posiadać obsługę przynajmniej takich protokołów przesyłania grupowego takich jak: 33. IGMP v1 34. IGMP v2 35. IGMP v3 36. IGMP proxy 37. MLD v1/2 38. MLD proxy 39. Przełącznik musi zapewniać możliwość konfiguracji interfejsów warstwy trzeciej, przynajmniej dla portów fizycznych, zagregowanych, interfejsów VLAN oraz interfejsów loopback. 40. Przełącznik musi zapewnić obsługę routingu bezklasowego IPv4 jak i routingu IPv6. 41. Przełącznik musi posiadać wsparcie funkcjonalności takich jak: 42. Routing dynamiczny RIPv2 43. Routing w oparciu o politykę. 44. Wbudowany serwer DHCP 45. DHCP relay w warstwie trzeciej. 46. Serwer DHCP musi przynajmniej posiadać możliwość stworzenia pul adresowych jak i statycznego przypisania adresu MAC do wskazanego adresu IP. 47. Przełącznik musi przynajmniej musi posiadać możliwość zarządzania za pomocą protokołów takich jak: 48. SSH 49. Port konsolowy 50. SSL 51. Przełącznik musi przynajmniej umożliwiać przeciwdziałanie burzom rozgłoszeniowym jak i multiemisyjnym. 52. Przełącznik musi posiadać ochronę przed podszywaniem się pod serwer DHCP. 53. Przełącznik musi posiadać ochronę protokołu ARP. 54. Przełącznik musi posiadać ochronę źródłowych adresów IP. 55. Przełącznik musi posiadać ochronę źródłowych adresów MAC. 56. Przełącznik musi posiadać możliwość uwierzytelniania przynajmniej za pomocą protokołów takich jak: 57. RADIUS 58. TACACS+ 59. 802.1X 60. Uwierzytelnianie oparte na sieci WWW za pośrednictwem przeglądarki internetowej klienta końcowego 61. Przełącznik musi posiadać ochronę przed atakami typu “odmowa usługi” 62. Przełącznik musi przynajmniej posiadać możliwość konfiguracji listy dostępowej, która umożliwiałaby blokowanie lub zezwalanie dostępu do urządzenia, bądź filtrowanie ruchu w oparciu o takie parametry jak: 63. Źródłowy adres MAC 64. Docelowy adres MAC 65. Źródłowy Adres IPv4/IPv6 66. Docelowy Adres IPv4/IPv6 67. Źródłowy port TCP/UDP 68. Docelowy port TCP/UDP 69. Flagi TCP 70. ICMP 71. Przełącznik musi umożliwiać konfigurację funkcjonalności QoS przynajmniej na poziomie wsparcia dla: 72. Ośmiu kolejek sprzętowych 73. SP 74. WRR 75. Mechanizmu unikania zatorów 76. Limitowania pasma 77. Optymalizacji ruchu dla protokołu iSCSI 78. Przełącznik musi posiadać możliwość badania stanu urządzenia za pomocą przynajmniej takich protokołów jak: 79. SNMP v1 80. SNMP v2 81. SNMP v3 82. Przełącznik musi posiadać możliwość pozyskiwania zdarzeń z urządzania przynajmniej za pomocą protokołu syslog. 83. Przełącznik musi posiadać wsparcie dla protokołu LLDP. 84. Przełącznik musi przynajmniej musi posiadać możliwość wybrania portu, na którym będzie działać protokołu LLDP. 85. Przełącznik musi przynajmniej musi posiadać możliwość wskazania czy dany port będzie wykorzystywany do wysyłania, odbierania lub do obustronnej transmisji pakietów LLDP na wskazanym porcie. 86. Przełącznik musi przynajmniej musi posiadać możliwość pobierania i wysyłania konfiguracji za protokołu TFTP. 87. Przełącznik musi posiadać wsparcie dla IPv6 w zakresie: 88. IPv6 QoS 89. IPv6 ACL 90. IPv6 First Hop Security 91. Aplikacji 92. Web/SSL 93. SSH 94. SNTP 95. TFTP 96. SNMP 97. RADIUS 98. TACACS+ 99. Panel administracyjny musi być dostępny z poziomu przeglądarki, zapewniając możliwość konfiguracji, monitorowania oraz konserwację przełącznika. 100. Wymagane jest wsparcie producenta na okres 12 miesięcy   **Do przełącznika należy dołączyć 12 wkładek SFP+ 10GB, 3 patchcordy światłowodowe**  **jednomodowe duplex LC-LC 5m, oraz 10 patchcordów światłowodowych jednomodowe duplex LC-LC 3m**. |

## Przełącznik sieci LAN IDF 2 szt.

|  |  |
| --- | --- |
| **Przełącznik sieciowy 48 portów** | 1. Przełącznik musi posiadać minimum 48 portów RJ45 o minimalnej prędkości 1 Gb/s. 2. Przełącznik musi posiadać minimum 4 portów SFP+ o prędkości minimum 10 Gb/s. 3. Przełącznik musi posiadać minimum 1 port RJ45 o minimalnej prędkości 1 Gb/s przeznaczony do zarządzania typu OOB. 4. Przełącznik musi posiadać porty konsolowe typu RJ-45 oraz USB typu C. 5. Przełącznik musi umożliwiać montaż w standardowej szafie rack 19”. 6. Przepustowość przełącznika nie może być mniejsza niż 176 Gb/s. 7. Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 130,94Mp/s, (pakiety wielkości 64 bajtów). 8. Przełącznik musi pozwalać na Stacking sprzętowy. 9. Wielkość bufora pakietów nie może być mniejsza niż 1,5 MB. 10. Przełącznik musi obsługiwać technologię drzewa rozpinającego w przynajmniej w wersji: 11. STP (IEEE 802.1d) 12. RSTP (IEEE 802. 1w) 13. MSTP (IEEE 802. 1s) 14. Przełącznik musi pozwalać na zabezpieczenie protokołu drzewa rozpinającego za pomocą: 15. BPDU 16. STP Root Guard 17. STP loopback guard 18. Przełącznik musi wspierać agregację portów przynajmniej w oparciu o protokół 802.3ad 19. Przełącznik musi posiadać wsparcie dla technologii 802.1Q. 20. Przełącznik musi posiadać wsparcie przynajmniej dla takich protokołów jak: 21. MAC VLAN 22. IP VLAN 23. Management VLAN 24. QinQ 25. Voice VLAN 26. VLANy prywatne 27. PVE 28. Multicast TV VLAN 29. Dynamiczne przydzielanie VLAN’ów w ramach uwierzytelniania oraz autoryzacji 802.1X/RADIUS 30. Przełącznik musi wspierać wykrywanie uszkodzeń warstwy pierwszej, które mogą powodować pętle. 31. Przełącznik musi zapewniać obsługę przekazywania ruchu DHCP pomiędzy VLAN’ami wraz z obsługa opcji 82. 32. Przełącznik musi posiadać obsługę przynajmniej takich protokołów przesyłania grupowego takich jak: 33. IGMP v1 34. IGMP v2 35. IGMP v3 36. IGMP proxy 37. MLD v1/2 38. MLD proxy 39. Przełącznik musi zapewniać możliwość konfiguracji interfejsów warstwy trzeciej, przynajmniej dla portów fizycznych, zagregowanych, interfejsów VLAN oraz interfejsów loopback. 40. Przełącznik musi zapewnić obsługę routingu bezklasowego IPv4 jak i routingu IPv6. 41. Przełącznik musi posiadać wsparcie funkcjonalności takich jak: 42. Routing dynamiczny RIPv2 43. Routing w oparciu o politykę. 44. Wbudowany serwer DHCP 45. DHCP relay w warstwie trzeciej. 46. Serwer DHCP musi przynajmniej posiadać możliwość stworzenia pul adresowych jak i statycznego przypisania adresu MAC do wskazanego adresu IP. 47. Przełącznik musi przynajmniej posiadać możliwość zarządzania za pomocą protokołów takich jak: 48. SSH 49. Port konsolowy 50. SSL 51. Przełącznik musi przynajmniej umożliwiać przeciwdziałanie burzom rozgłoszeniowym jak i multiemisyjnym. 52. Przełącznik musi posiadać ochronę przed podszywaniem się pod serwer DHCP. 53. Przełącznik musi posiadać ochronę protokołu ARP. 54. Przełącznik musi posiadać ochronę źródłowych adresów IP. 55. Przełącznik musi posiadać ochronę źródłowych adresów MAC. 56. Przełącznik musi posiadać możliwość uwierzytelniania przynajmniej za pomocą protokołów takich jak: 57. RADIUS 58. TACACS+ 59. 802.1X 60. Uwierzytelnianie oparte na sieci WWW za pośrednictwem przeglądarki internetowej klienta końcowego 61. Przełącznik musi posiadać ochronę przed atakami typu “odmowa usługi” 62. Przełącznik musi przynajmniej posiadać możliwość konfiguracji listy dostępowej, która umożliwiałaby blokowanie lub zezwalanie dostępu do urządzenia, bądź filtrowanie ruchu w oparciu o takie parametry jak: 63. Źródłowy adres MAC 64. Docelowy adres MAC 65. Źródłowy Adres IPv4/IPv6 66. Docelowy Adres IPv4/IPv6 67. Źródłowy port TCP/UDP 68. Docelowy port TCP/UDP 69. Flagi TCP 70. ICMP 71. Przełącznik musi umożliwiać konfigurację funkcjonalności QoS przynajmniej na poziomie wsparcia dla: 72. Ośmiu kolejek sprzętowych 73. SP 74. WRR 75. Mechanizmu unikania zatorów 76. Limitowania pasma 77. Optymalizacji ruchu dla protokołu iSCSI 78. Przełącznik musi posiadać możliwość badania stanu urządzenia za pomocą przynajmniej takich protokołów jak: 79. SNMP v1 80. SNMP v2 81. SNMP v3 82. Przełącznik musi posiadać możliwość pozyskiwania zdarzeń z urządzania przynajmniej za pomocą protokołu syslog. 83. Przełącznik musi posiadać wsparcie dla protokołu LLDP. 84. Przełącznik musi przynajmniej posiadać możliwość wybrania portu, na którym będzie działać protokołu LLDP. 85. Przełącznik musi przynajmniej posiadać możliwość wskazania czy dany port będzie wykorzystywany do wysyłania, odbierania lub do obustronnej transmisji pakietów LLDP na wskazanym porcie. 86. Przełącznik musi przynajmniej posiadać możliwość pobierania i wysyłania konfiguracji za protokołu TFTP. 87. Przełącznik musi posiadać wsparcie dla IPv6 w zakresie: 88. IPv6 QoS 89. IPv6 ACL 90. IPv6 First Hop Security 91. Aplikacji 92. Web/SSL 93. SSH 94. SNTP 95. TFTP 96. SNMP 97. RADIUS 98. TACACS+ 99. Panel administracyjny musi być dostępny z poziomu przeglądarki, zapewniając możliwość konfiguracji, monitorowania oraz konserwację przełącznika. 100. Wymagane jest wsparcie producenta na okres 12 miesięcy |

## Access Point 5 szt.

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   1. Temperatura 0–50°C,
   2. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
   1. 2.4 GHz 802.11b/g/n,
   2. 5 GHz 802.11a/n/ac/ax,
   3. Skaner 2.4GHz i 5GHz
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX,
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   1. Tunnel,
   2. Bridge,
   3. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    1. MIMO – 2x2,
    2. Maksymalna przepustowość dla poszczególnych modułów radiowych:
       1. 574 Mbps;
       2. 1201 Mbps;
    3. Wymagana moc nadawania:
       1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
       2. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    4. Wsparcie dla 802.11n 20/40Mhz HT,
    5. Wsparcie dla kanałów 80MHz,
    6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
    7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
    8. Maksymalna deklarowana liczba klientów per moduł radiowy:
       1. 512;
       2. 512;
12. Funkcje dodatkowe:
    1. OFDMA UL i DL
    2. Spatial Reuse (BSS Coloring)
    3. UL-MU-MIMO 802.11ax
    4. DL-MU-MIMO
    5. Enhanced Target Wake Time (TWT)

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

## Instalacja, konfiguracja, wdrożenie, utrzymanie części II

Wykonawca będzie odpowiedzialny za pomoc w wdrożeniu następujących rozwiązań:

Firewall: Instalacja i konfiguracja zapór ogniowych w celu ochrony sieci przed nieautoryzowanym dostępem.

Centralny system logów: Instalacja narzędzi do centralnego gromadzenia i analizy logów systemowych, co pomoże w wykrywaniu nieprawidłowości i incydentów bezpieczeństwa.

Środowisko WiFi: Wdrożenie infrastruktury sieciowej WiFi, obejmującej zarówno sprzęt, jak i konfigurację.

# Część III

## System EDR-XDR

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.

2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.

3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego

identyfikatora sprzętowego stacji.

5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli

administracyjnej.

8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co

najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami

administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz

oraz brak.

9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.

10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić

klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP,

aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły

komputera.

12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem:

wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia

oraz umieszczeniu agenta w grupie dynamicznej.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware,

dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem

komputera do sieci botnet.

5. Rozwiązanie musi posiadać funkcjonalność przywrócenie plików po ich zaszyfrowaniu przez

oprogramowanie typu ransomware.

6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz

podejrzanych aplikacji.

7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i

wykonywanych plików.

8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików

"na żądanie" lub według harmonogramu.

9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków

sieciowych i dysków przenośnych.

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

11. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

12. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

14. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

16. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

18. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

19. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

20. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

21. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

23. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.

24. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

25. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

26. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

27. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

28. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

29. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

30. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

31. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona stacji roboczych - macOS**

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych.

2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM)

3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.

5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.

8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

9. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.

10. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

**Ochrona stacji roboczych – Linux**

1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint.

2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.

3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.

4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.

7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.

10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

5. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO).

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

a. nazwę aplikacji,

b. nazwę pakietu,

c. kategorię sklepu Google Play,

d. uprawnienia aplikacji,

e. pochodzenie aplikacji z nieznanego źródła.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.

5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.

8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.

11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

a) Czysty,

b) Podejrzany,

c) Bardzo podejrzany,

d) Szkodliwy.

13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Moduł XDR**

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

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

7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

## Oprogramowanie do zarządzania siecią IT – aktualizacja licencji do 300 szt.

Zamawiający oczekuje zwiększenia liczby licencji z 200 szt. do 300 szt. oprogramowania w formie bezterminowej z serwisem i wsparciem na 12 miesięcy, zgodnego z poniższą specyfikacją

1. Oprogramowanie musi posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program ma umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.
2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.
3. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.
5. Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityk pozawala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.
6. Program zawiera mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.
7. Producent został wyróżniony znakiem jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).
8. MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

* wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
* wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją OU)
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
* wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
* wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
* wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
* zablokowania mapy urządzeń przed przypadkową edycją
* serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
* serwerów pocztowych:

- program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty

- program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)

- program ma możliwość wykonywania operacji testowych

- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa

* monitorowania serwerów WWW i adresów URL
* cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
* obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
* obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
* obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
* monitoringu routerów i przełączników wg:

- zmian stanu interfejsów sieciowych

- ruchu sieciowego

- podłączonych stacji roboczych – graficzna prezentacja panelu switcha

- ruchu generowanego przez podłączone do portów stacje robocze

* serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
* wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
* monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
* zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
* wydajności systemów Windows:

- obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

1. Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program musi posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
2. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0
3. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

WZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

* Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
* Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
* Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
* Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio
* umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
* Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
* Musi posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania
* programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
* Umożliwia odczytanie numeru seryjnego (klucze licencyjne).
* Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
* Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych
* środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
* Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
* Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

* przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
* przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
* tworzenia powiązań między zasobami a urządzeniami,
* tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
* wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
* definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
* określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
* określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
* masową edycję atrybutów zasobów,
* definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
* importu danych z zewnętrznego źródła (.CSV),
* przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
* tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
* oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
* ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
* generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
* przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
* konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
* konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
* archiwizacji i porównywania audytów zasobów,
* tworzenia kodów kreskowych dla zasobów,
* drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
* inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
* możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
* inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
* definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji

o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie

archiwów ZIP.

2. Informacje o aplikacjach używanych w organizacji.

3. Tworzenie własnych wzorców aplikacji.

4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

5. Informacje o komputerach, na których aplikacja została wykryta.

6. Zarządzanie posiadanymi licencjami.

7. Wskazywanie osób odpowiedzialnych za licencję.

8. Wskazanie użytkowników licencji.

9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby musi posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.

13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe muszą posiadać możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

* Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
* Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
* Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
* Informacji o edytowanych przez użytkownika dokumentach,
* Historii pracy (cykliczne zrzuty ekranowe),
* Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
* Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
* Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
* Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto musi posiadać możliwość:

* wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy.
* zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
* wyszczególnienia podejrzanej aktywności w raportach.
* wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
* automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
* blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
* integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
* skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
* automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
* blokowania ruchu na wskazanych portach TCP/IP,
* blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
* prowadzenia rejestru naruszeń blokad,
* wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
* przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
* definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich

komputerach pracowali w danym czasie.

Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

Program musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania

użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.

W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów

technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.

Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie

rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:

* zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
* rozmowy również między „zwykłymi” użytkownikami
* przesyłanie plików między rozmówcami w trybie online
* tworzenie pokojów tematycznych, rozmów grupowych
* oznaczanie kontaktów jako „ulubionych” na liście kontaktów
* uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
* może być wyświetlany w trybie jasnym lub ciemnym

W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać

najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów

(opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii

odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość

tworzenia szkiców i archiwizowania komunikatów.

Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do

swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu

przez każdego pracownika.

Moduł pomocy zdalnej umożliwia również:

* pobieranie listy użytkowników z Active Directory,
* wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
* zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
* zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
* tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
* automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
* definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
* przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
* procesowanie zgłoszeń użytkowników z wiadomości e-mail,
* eksportowania listy zgłoszeń do plików CSV i XLSX,
* integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
* tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
* wykonywanie operacji na wielu zgłoszeniach równocześnie,
* dołączanie załączników do zgłoszeń,
* rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
* szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
* wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
* zrzuty ekranowe (podgląd pulpitu),
* zdalną modyfikację rejestrów,
* dystrybucję oprogramowania przez Agenty,
* definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
* przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
* dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
* zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
* możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
* możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
* planowanie nieobecności pracowników helpdesk,
* obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
* generowanie raportów obsługi helpdesk,
* zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
* zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
* wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Kolejną funkcją oprogramowania jest MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia

(drukarka, klawiatura, mysz itp.) mogą być podłączane.

5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.

7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków

BitLocker.

8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.

9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.

10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie

odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.

11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym

oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.

12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.

3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

## Instalacja, konfiguracja, wdrożenie, utrzymanie części III

EDR/XDR: Instalacja rozwiązań zabezpieczających, takich jak Endpoint Detection and Response (EDR) oraz Extended Detection and Response (XDR), które pomagają w wykrywaniu i reagowaniu na zagrożenia w czasie rzeczywistym.

Oprogramowanie do zarządzania siecią IT: Wdrożenie narzędzi do monitorowania i zarządzania całą infrastrukturą sieciową, w tym rozwiązań do analizy ruchu sieciowego, zarządzania konfiguracją urządzeń sieciowych oraz monitorowania dostępności usług.

# Część IV

## System SIEM-SOAR

**Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności.**

1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.

2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.

3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.

4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;

5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.

6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.

7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.

8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.

9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.

10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.

12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.

13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.

14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.

15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.

18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.

20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.

21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.

22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.

24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.

26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.

27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.

28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

1. nowe zasoby wykryte w sieci,
2. typy wykrytych zasobów (np.: serwer lub stacja robocza),
3. zastosowane na nich zabezpieczenia,
4. usługi z którymi się komunikują,
5. nowe usługi wykryte na zasobie
6. komunikację do usług wykrytych na zasobie.

30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.

31. System powinien musi posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.

32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.

33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

1. fqdn,
2. e-mail,
3. nazwa pliku,
4. ścieżka do pliku,
5. hash,
6. adres IP,
7. klucz rejestru,
8. cmd.

34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).

35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).

36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).

37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).

40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.

41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.

42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.

43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:

1. id techniki,
2. taktykę,
3. platformy których dotyczy,
4. potencjalne źródła,
5. opis zagrożenia,
6. mityzację,
7. sposób detekcji,
8. referencje.

44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).

46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:

1. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
2. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
3. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
4. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.

49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.

52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:

1. sparsowane pola oraz ich wartości,
2. listy referencyjne,
3. atrybuty użytkowników z Active Directory,
4. atrybuty komputerów z Active Directory,
5. bazę wskaźników kompromitacji (IOC),
6. informacje z elektronicznej dokumentacji,
7. anomalie w zachowaniu użytkowników (UBA),
8. anomalie w zachowaniu zasobów (EBA),
9. podatności na zasobach,
10. wyniki analizy konfiguracji,
11. techniki MITRE ATT&CK®,

53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:

1. wykrycie dowolnej treści w logach,
2. wykrycie zmiany jednego z kilku pól,
3. wykrycie zaniku wiadomości,
4. wykrycie nowej wartości pola w zadanym okresie czasu,
5. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
6. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
7. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
8. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
9. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
10. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
11. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
12. wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
13. wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

1. wykrycie wystąpienia wartości pola na wybranej liście,
2. wykrycie niewystępowania wartości pola na wybranej liście,
3. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony),
4. wykrycie niewystąpienia pary wartości na wybranej liście
5. (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).

55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

1. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
2. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
3. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
4. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
5. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

1. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
2. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
3. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

1. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
2. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
3. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:

1. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
2. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
3. wykrycie nieautoryzowanej usługi na serwerze,
4. wykrycie nieautoryzowanego połączenia do usługi na serwerze,
5. wykrycie nieautoryzowanego połączenia z serwera usług,
6. wykrycie nieautoryzowanego połączenia do sieci Internet.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

1. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
2. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
3. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
4. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

1. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
2. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
3. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
4. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

1. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
2. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
3. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności,
4. wykrycie zdarzeń o wysokim „severity” do zasobów posiadającego krytyczne podatności.

62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:

1. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
2. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

1. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
2. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
3. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

1. wykrycie anomalii na koncie uprzywilejowanym użytkownika,
2. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
3. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
4. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
5. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

1. sparsowane pola oraz ich wartości,
2. atrybuty użytkowników z Active Directory,
3. atrybuty komputerów z Active Directory,
4. informacje z elektronicznej dokumentacji.

66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

1. adresie IP,
2. koncie domenowym użytkownika,
3. strefie bezpieczeństwa,
4. zakresie adresów IP.

67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.

1. wszystkie skorelowane zdarzenia,
2. korespondencja pocztowa,
3. załączniki z próbkami lub dowodami,
4. wskaźniki kompromitacji (IoC),
5. informacje pozyskane z innych systemów.

70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

1. identyfikację celu i źródła zagrożenia,
2. nazwę oraz adres IP źródła zagrożenia,
3. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
4. lokalizację z które pochodzi zagrożenie np.: Internet,
5. strefę bezpieczeństwa z której pochodzi zagrożenie,
6. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
7. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
8. nazwę oraz adres IP celu zagrożenia,
9. zabezpieczenia lokalne chroniące cel zagrożenia,
10. strefę bezpieczeństwa w której znajduje się cel zagrożenia.

73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

1. nazwy zasobu,
2. rodzaju zasobu,
3. ważności zasobu dla organizacji,
4. rodzaj przetwarzanych informacji,
5. usług, które ten zasób świadczy,
6. lokalizację użytkowników, którzy z niego korzystają,
7. usługi z których zasób korzysta.

76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

1. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
2. segregacja – segregacja i kwalifikacja zdarzeń,
3. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
4. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
5. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

1. podgląd aktywności zagrożonego zasobu na linii czasu,
2. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
3. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
4. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
5. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
6. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
7. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:
   * listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
   * listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
8. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:
   * listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
   * listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

1. warunki powiadomień,
   * zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
   * zdarzeń o przekroczonych czasach SLA o definiowalny okres,
   * zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
   * zdarzeń, których priorytet osiągnął określoną wartość,
   * zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
   * zdarzeń na których doszło do naruszenia bezpieczeństwa,
   * zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
   * zdarzeń realizujących zdefiniowaną usługę,
   * zdarzeń przetwarzających sklasyfikowane informację,
   * zdarzeń przetwarzanych na krytycznych zasobach,
2. odbiorców powiadomień, w tym:
   * operatora, któremu zostało przydzielone zdarzenie,
   * właściciela zasobu na którym wystąpiło zdarzenie,
   * zespół obsługi, który odpowiada za obsługę zdarzeń,
   * właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
   * podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
3. kanały powiadomień, m.in. e-mail, sms, komunikator,
4. zastosowanie mechanizmów grupowania:
   * grupowanie wielu powiadomień w jednej wiadomości,
   * ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

1. utworzenia nowego zdarzenia z określonym priorytetem,
2. utworzenia nowego zdarzenia na zasobie krytycznym,
3. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
4. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
5. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
6. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora,
7. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
8. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.

87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

1. wybór raportu, który ma zostać wysłany,
2. zdefiniowanie jego tytułu,
3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
4. możliwość ograniczenia cyklu do dni powszednich,
5. określenie daty przesłania pierwszego raportu,
6. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
   * zdefiniowanej daty końcowej,
   * określnej liczby raportów,
7. określenie odbiorców raportu.

88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

1. strefę bezpieczeństwa w której została wykryta podatność,
2. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
3. rodzaj zasobu którego dotyczy ta podatność,
4. ważność tego zasobu dla organizacji,
5. przetwarzane na tym zasobie informacje, np.: dane osobowe,
6. usługi realizowane przez ten zasób, np.: DNS,
7. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
8. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
9. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

1. wyliczonym priorytecie podatności,
2. aktualnym statusie obsługi,
3. ważności zasobu na którym została wykryta,
4. adresie IP tego systemu,
5. parametrów SLA związanych z tym statusem,
6. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
7. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

1. przekroczenia czasu reakcji o określony czas np.: o godzinę,
2. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
3. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
4. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
5. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
6. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
7. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
8. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
9. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
10. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
11. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,

93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

1. warunki powiadomień,
   * podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
   * podatności o przekroczonych czasach SLA o definiowalny okres,
   * podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
   * podatności, których priorytet osiągnął określoną wartość,
   * zdarzeń realizujących zdefiniowaną usługę,
   * zdarzeń przetwarzających sklasyfikowane informację,
   * zdarzeń przetwarzanych na krytycznych zasobach,
2. odbiorców powiadomień, w tym:
   * operatora, któremu została przydzielona podatność,
   * właściciela zasobu na którym wystąpiła podatność,
   * zespół obsługi, który odpowiada za obsługę podatności,
   * właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
   * podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
3. kanały powiadomień, m.in. e-mail, sms, komunikator,
4. zastosowanie mechanizmów grupowania:
   * grupowanie wielu powiadomień w jednej wiadomości,
   * ograniczenie liczby wierszy powiadomienia do określonej wartości.

94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

1. przydzielenia nowej podatności do obsługi z określonym priorytetem,
2. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
3. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
4. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
5. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
6. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
7. przejęcia przydzielonej operatorowi podatności przez innego operatora.

95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

1. wybór raportu który ma zostać wysłany,
2. zdefiniowanie jego tytułu,
3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
4. możliwość ograniczenia cyklu do dni powszednich,
5. określenie daty przesłania pierwszego raportu,
6. określenie okresu przez jaki będą one przesyłane, poprzez:
   * zdefiniowanie daty końcowej,
   * bez daty końcowej,
   * określenie liczby raportów,
7. określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.

97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:

1. zestaw wykresów dla bieżącego użytkownika,
2. zestaw wykresów dla wybranego użytkownika,
3. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
4. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:

1. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
   * ilość zdarzeń nowych i niesklasyfikowanych,
   * ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
   * ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
2. wykres przedstawiający skale zagrożeń, który uwzględnia:
   * ilość zasobów krytycznych na których są obsługiwane zdarzenia,
   * ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
3. wykres przedstawiający źródła zagrożeń, który uwzględnia:
   * ilość nowych zdarzeń dotyczących użytkowników,
   * ilość podjętych zdarzeń dotyczących użytkowników,
   * ilość nowych zdarzeń dotyczących zasobów,
   * ilość podjętych zdarzeń dotyczących zasobów,
4. wykres przedstawiający poziom zagrożeń, który uwzględnia:
   * ilość nowych zdarzeń w podziale na priorytety,
   * ilość podjętych zdarzeń w podziale na priorytety,
5. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
   * ilość zdarzeń zarejestrowanych w bieżącym dniu,
   * ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
   * ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
   * ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
6. wykres przedstawiający zagrożone usługi, który uwzględnia:
   * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
   * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
7. wykres przedstawiający zagrożone dane, który uwzględnia:
   * ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
   * ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
   * ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
   * ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
8. wykres przedstawiający skale podatności, który uwzględnia:
   * ilość zasobów krytycznych na których są obsługiwane podatności,
   * ilość zasobów niekrytycznych na których są obsługiwane podatności,
9. wykres przedstawiający czas obsługi podatności, który uwzględnia:
   * ilość podatności zarejestrowanych w bieżącym dniu,
   * ilość podatności zarejestrowanych w ostatnim tygodniu,
   * ilość podatności zarejestrowanych w ostatnim miesiącu,
   * ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
10. wykres przedstawiający wagę podatności, który uwzględnia:
    * ilość nowych podatności w podziale na priorytety,
    * ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:

1. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
2. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
3. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
4. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
5. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
6. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

a. kolektor parsujący;

b. kolektor logów;

c. kolektor korelacyjny;

d. kolektor zdarzeń;

e. kolektor sztucznej inteligencji;

f. kolektor reakcyjny;

g. kolektor kontrolujący.

102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz musi posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz musi posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.

112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.

117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

a. zdolność do definiowania wzorców które powtarzają się jako zmienne;

b. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;

c. zdolność do testowania poszczególnych funkcji;

d. zdolność do przekształcania danych w trakcie ich parsowania.

126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

a. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;

b. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;

c. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;

d. zdolność do monitorowania integralności plików;

e. zdolność do monitorowania rejestru systemowego;

f. zdolność do monitorowania urządzeń zewnętrznych (removable devices);

g. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;

h. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;

i. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;

j. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi

132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.

133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.

134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.

135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.

136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 5 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć.

139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub musi posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.

141. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

142. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

143. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

144. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).

145. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

146. Wykonawca zapewni szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 5 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

147. Produkt musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać 350 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

## Instalacja, konfiguracja, wdrożenie, utrzymanie części IV

Szczegółowy zakres i wytyczne procesu wdrożenia systemu, instalacji i konfiguracji:

1. Proces wdrożenia systemu określony w Etapie I powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w okresie 4 miesięcy.

2. Proces wdrożeniowy podzielony zostanie są na 2 obszary:

a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);

b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;

c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR;

d. Obszar Danych Osobowych, zakładający zainstalowanie i skonfigurowanie modułu Ochrony Danych Osobowych i jego integracji z pozostałymi modułami systemu (tj. SIEM i SOAR).

3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:

a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);

b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:

• konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,

• instalację lub import maszyny wirtualnej typu „software appliance”,

• zestawienie połączenia zdalnego,

• aktywację licencji,

• wstępną konfigurację,

• import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);

c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:

• przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,

• uruchomienie reguł wykrywania;

d. Prace audytowe, w tym:

• pasywną analizę transmisji sieciowej:

o ruch z/do serwerów webowych i aplikacyjnych,

o ruch z/do serwerów baz danych,

o ruch z/do serwerów pocztowych,

o ruch z/do kontrolerów domenowych,

o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),

o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,

• konsultacje w ramach otrzymanych wyników;

• zebranie danych audytowych wymaganych do sporządzenia raportu;

e. Analizę podatności, w zakresie:

• integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;

• przygotowanie reguł priorytetów i importu krytycznych podatności;

f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:

• zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;

• potencjalne wektory ataków dla wykrytych zagrożeń;

• wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;

• rekomendacja zabezpieczeń;

• zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;

g. Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

a. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:

• zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);

• sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)

• centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);

• kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;

• systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);

• system SIEM

• w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;

b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;

c. Podłączenie reguł detekcji;

d. Podłączenie i konfiguracja mechanizmów UEBA:

• integracja z Active Directory

• utworzenie profili użytkowników UBA

• utworzenie profili hostów EBA

• import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia

• obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów.

d. Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;

5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać kolejno:

a. Pracę z konsultantem (m.in wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian związanych z dostosowaniem scenariuszy, pomoc przy generowaniu API KEY dla wbudowanych akcji)

b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi

c. Konfigurację mechanizmów powiadamiania