Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Specyfikacja techniczna

Niniejszy załącznik stanowi szczegółowy opis przedmiotu zamówienia. Zaoferowane przez Wykonawcę rozwiązania muszą spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Wymagane minimalne parametry techniczne".

Wykonawca zobowiązany jest podać w formularzu oferty producenta, model/wersję oferowanego rozwiązania, typ dzięki czemu będzie można jednoznacznie określić jaki produkt został zaoferowany. Dodatkowo Zamawiający dopuszcza podanie linków dostępowych dla oferowanego n/w sprzętu dostępnych na stronach internetowych producentów.

Spis treści

1. Szkolenia dla administratorów

Wykonawca przeprowadzi szkolenia w zakresie EDR i skanera podatności dla działu IT JST. Szkolenia powinny odbywać się w grupach i trwać nie krócej niż 4h. Szkolenia przeprowadzone będą w siedzibie Zamawiającego tj. w budynku JST Wykonawca przekaże harmonogram szkolenia nie później niż 7 dni przed rozpoczęciem szkolenia.

Dla zapewnienia wysokiego poziomu usług podmiot prowadzący szkolenie musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie usług szkoleniowych oraz usług związanych z cyberbezpieczeństwem – certyfikaty należy załączyć do oferty.

1.1. Program szkolenia:

1.1.1.1. Różnice między antywirusem, a EDRem

1.1.1.2. W jaki sposób można poprawić bezpieczeństwo

1.1.1.3. Dlaczego jeden alert to za mało

1.1.1.4. Jak wykrywać luki bezpieczeństwa

1.1.1.5. Zarządzanie naprawą luk bezpieczeństwa

1.1.2. Wykrywanie i reagowanie

1.1.2.1. Rozpoznawanie szerszego kontekstu

1.1.2.2. Reagowanie na incydenty

1.1.2.3. Zarządzanie przeanalizowanymi incydentami

1.1.3. Reakcja na incydent bezpieczeństwa

1.1.3.1. Rozpoznanie incydentu bezpieczeństwa

1.1.3.2. Separacja zainfekowanego urządzenia

1.1.3.3. Analiza drogi atakującego

1.1.3.4. Analiza uruchomionych procesów

1.1.3.5. Analiza komend w skryptach

1.1.3.6. Powstrzymywanie incydentu

1.1.3.7. Naprawa uszkodzeń

1.1.4. Przykłady zagrożeń

1.1.4.1. Wykrycie trwałego ataku

1.1.4.2. Ruchy poprzeczne

1.1.4.3. Zwiększenie uprawnień

1.1.4.4. Modyfikacja składników systemowych

1.1.4.5. Modyfikacja programów

1.1.4.6. Działania wywiadowcze

1.1.4.7. Modyfikacja poufnych informacji

1.1.5. Skanowanie podatności

1.1.5.1. Wykrywanie urządzeń

1.1.5.2. Wykrywanie otwartych portów

1.1.5.3. Sprawdzanie "jak nas świat widzi"

1.1.5.4. Wykrywanie luk bezpieczeństwa

1.1.5.5. Okresowe sprawdzanie luk bezpieczeństwa

1.1.6. Zarządzanie naprawą luk bezpieczeństwa

1.1.6.1. Ustalanie priorytetu i ważności luk

1.1.6.2. Aktualizacja oprogramowania

1.1.6.3. Przekonfigurowanie oprogramowania

1.1.6.4. Zamykanie otwartych portów

2. Urządzenia serwerowe

2.1. Serwer TYP I – 1 szt.

2.1.1. Obudowa

2.1.1.1. Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5”

2.1.1.2. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.

2.1.1.3. 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.

2.1.2. Płyta główna

2.1.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów.

2.1.2.2. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci.

2.1.2.3. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

2.1.2.4. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

2.1.2.5. Możliwość obsługi procesorów 32 rdzeniowych

2.1.3. Chipset

2.1.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

2.1.4. Procesor

2.1.4.1. Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.1GHz, klasy x86, dedykowany do pracy z zaoferowanym serwerem **,** umożliwiający osiągnięcie wyniku min. 168 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

2.1.5. RAM

2.1.5.1. Minimum 64GB DDR4 RDIMM 3200MT/s

2.1.6. Funkcjonalność pamięci RAM

2.1.6.1. Advanced ECC,

2.1.6.2. Memory Page Retire,

2.1.6.3. Fault Resilient Memory,

2.1.6.4. Memory Self-Healing lub PPR,

2.1.6.5. Partial Cache Line Sparing

2.1.7. Kontroler RAID

2.1.7.1. Sprzętowy kontroler dyskowy, posiadający

2.1.7.1.1. Min. 8GB nieulotnej pamięci cache,

2.1.7.1.2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.

2.1.7.1.3. Wsparcie dla dysków samoszyfrujących.

2.1.8. Dyski twarde

2.1.8.1. Zainstalowane:

2.1.8.1.1. 6x dysk SSD SATA o pojemności min. 960GB, 2,5“ Hot-Plug.

2.1.8.2. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.

2.1.8.3. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

2.1.9. Zasilacze

2.1.9.1. Redundantne, Hot-Plug min. 700W klasy Titanium

2.1.10. Gniazda PCI

2.1.10.1. minimum jeden slot PCIe

2.1.11. Interfejsy sieciowe/FC/SAS

2.1.11.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

2.1.12. Porty

2.1.12.1. 4x USB w tym przynajmniej 1x USB 3.0

2.1.12.2. 2x VGA w tym jedno z przodu serwera

2.1.13. System operacyjny/System wirtualizacji

2.1.13.1. Microsoft Windows Server 2022 Standard

2.1.14. Elementy montażowe

2.1.14.1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych

2.1.15. Video

2.1.15.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

2.1.16. Bezpieczeństwo

2.1.16.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

2.1.16.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

2.1.16.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

2.1.16.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

2.1.16.5. Moduł TPM 2.0 V3

2.1.16.6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera

2.1.16.7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

2.1.16.8. 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).

2.1.17. Karta Zarządzania

2.1.17.1. Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

2.1.17.1.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

2.1.17.1.2. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

2.1.17.1.3. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera

2.1.17.1.4. wsparcie dla Public Key Authentication (PKA) over SSH

2.1.17.1.5. oraz z możliwością rozszerzenia funkcjonalności o:

2.1.17.1.6. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

2.1.17.1.7. szyfrowane SSL

2.1.17.1.8. wsparcie dla IPv6;

2.1.17.1.9. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

2.1.17.1.10. integracja z Active Directory;

2.1.17.1.11. wsparcie dla dynamic DNS;

2.1.17.1.12. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

2.1.17.1.13. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

2.1.17.1.14. możliwość obsługi przez sześciu użytkowników jednocześnie;

2.1.17.1.15. możliwość podmontowania zdalnych wirtualnych napędów;

2.1.17.1.16. wirtualną konsolę z dostępem do myszy, klawiatury;

2.1.17.1.17. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

2.1.17.1.18. Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej

2.1.17.1.19. Przesyłanie danych telemetrycznych w czasie rzeczywistym

2.1.17.1.20. Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze

2.1.17.1.21. Automatyczna rejestracja certyfikatów (ACE)

2.1.18. Oprogramowanie do zarządzania

2.1.18.1. Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

2.1.18.1.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych

2.1.18.1.2. integracja z Active Directory

2.1.18.1.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta

2.1.18.1.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish

2.1.18.1.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

2.1.18.1.6. Szczegółowy opis wykrytych systemów oraz ich komponentów

2.1.18.1.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF

2.1.18.1.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

2.1.18.1.9. Grupowanie urządzeń w oparciu o kryteria użytkownika

2.1.18.1.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

2.1.18.1.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach

2.1.18.1.12. Szybki podgląd stanu środowiska

2.1.18.1.13. Podsumowanie stanu dla każdego urządzenia

2.1.18.1.14. Szczegółowy status urządzenia/elementu/komponentu

2.1.18.1.15. Generowanie alertów przy zmianie stanu urządzenia.

2.1.18.1.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń

2.1.18.1.17. Integracja z service desk producenta dostarczonej platformy sprzętowej

2.1.18.1.18. Możliwość przejęcia zdalnego pulpitu

2.1.18.1.19. Możliwość podmontowania wirtualnego napędu

2.1.18.1.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów

2.1.18.1.21. Możliwość importu plików MIB

2.1.18.1.22. Przesyłanie alertów „as-is” do innych konsol firm trzecich

2.1.18.1.23. Możliwość definiowania ról administratorów

2.1.18.1.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

2.1.18.1.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

2.1.18.1.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta

2.1.18.1.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

2.1.18.1.28. 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.

2.1.18.1.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

2.1.18.1.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

2.1.18.1.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

2.1.18.1.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

2.1.18.1.33. Zdalne uruchamianie diagnostyki serwera.

2.1.18.1.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

2.1.18.1.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

2.1.19. Wspierane systemy operacyjne

2.1.19.1. Canonical® Ubuntu® Server LTS

2.1.19.2. Citrix® Hypervisor®

2.1.19.3. Microsoft® Windows Server® with Hyper-V

2.1.19.4. Red Hat® Enterprise Linux

2.1.19.5. SUSE® Linux Enterprise server

2.1.19.6. VMware® ESXi®

2.1.20. Certyfikaty

2.1.20.1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

2.1.20.2. Serwer musi posiadać deklaracja CE.

2.1.20.3. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.

2.1.20.4. 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 Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.

2.1.20.5. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

2.1.21. Dokumentacja użytkownika

2.1.21.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

2.1.21.2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2.1.22. **Wsparcie techniczne i oprogramowanie** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania

2.1.22.1. Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego,

2.1.22.2. automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.

2.1.22.3. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.

2.1.22.4. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.

2.1.22.5. 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.

2.1.22.6. 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.

2.1.22.7. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :

2.1.22.7.1. Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.

2.1.22.7.2. Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.

2.1.22.7.3. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.

2.1.22.7.4. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,

2.1.22.7.5. 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.

2.1.22.7.6. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne

2.1.22.7.7. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.

2.1.22.7.8. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)

2.1.22.7.9. sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)

2.1.22.7.10. dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml

2.1.22.7.11. 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.

2.1.23. Warunki gwarancji

2.1.23.1. Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres 3 lat.

2.1.23.2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

2.1.23.3. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)

2.1.23.4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

2.1.23.5. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

2.1.23.6. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

2.1.23.7. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

2.1.23.8. 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

2.1.23.9. 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.

2.1.23.10. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2.1.23.11. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

2.2. Serwer TYP II – 2 szt.

2.2.1. Obudowa

2.2.1.1. Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5”

2.2.1.2. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.

2.2.1.3. 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.

2.2.2. Płyta główna

2.2.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów.

2.2.2.2. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci.

2.2.2.3. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

2.2.2.4. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

2.2.2.5. Możliwość obsługi procesorów 32 rdzeniowych

2.2.3. Chipset

2.2.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

2.2.4. Procesor

2.2.4.1. Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.1GHz, klasy x86, dedykowany do pracy z zaoferowanym serwerem , umożliwiający

osiągnięcie wyniku min. 168 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

2.2.5. RAM

2.2.5.1. Minimum 64GB DDR4 RDIMM 3200MT/s

2.2.6. Funkcjonalność pamięci RAM

2.2.6.1. Advanced ECC,

2.2.6.2. Memory Page Retire,

2.2.6.3. Fault Resilient Memory,

2.2.6.4. Memory Self-Healing lub PPR,

2.2.6.5. Partial Cache Line Sparing

2.2.7. Kontroler RAID

2.2.7.1. Sprzętowy kontroler dyskowy, posiadający:

2.2.7.1.1. Min. 8GB nieulotnej pamięci cache,

2.2.7.1.2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.

2.2.7.1.3. Wsparcie dla dysków samoszyfrujących.

2.2.8. Dyski twarde

2.2.8.1. Zainstalowane:

2.2.8.1.1. 4x dysk SSD SATA o pojemności min. 960GB, 2,5“ Hot-Plug.

2.2.8.2. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.

2.2.8.3. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

2.2.9. Zasilacze

2.2.9.1. Redundantne, Hot-Plug min. 700W klasy Titanium

2.2.10. Gniazda PCI

2.2.10.1. minimum jeden slot PCIe

2.2.11. Interfejsy sieciowe/FC/SAS

2.2.11.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

2.2.12. Porty

2.2.12.1. 4x USB w tym przynajmniej 1x USB 3.0

2.2.12.2. 2x VGA w tym jedno z przodu serwera

2.2.13. System operacyjny/System wirtualizacji

2.2.13.1. Microsoft Windows Server 2022 Standard

2.2.14. Elementy montażowe

2.2.14.1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych

2.2.15. Video

2.2.15.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

2.2.16. Bezpieczeństwo

2.2.16.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

2.2.16.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

2.2.16.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

2.2.16.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

2.2.16.5. Moduł TPM 2.0 V3

2.2.16.6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera

2.2.16.7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

2.2.16.8. 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).

2.2.17. Karta Zarządzania

2.2.17.1. Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

2.2.17.1.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

2.2.17.1.2. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

2.2.17.1.3. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera

2.2.17.1.4. wsparcie dla Public Key Authentication (PKA) over SSH

2.2.17.1.5. oraz z możliwością rozszerzenia funkcjonalności o:

2.2.17.1.6. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

2.2.17.1.7. szyfrowane SSL

2.2.17.1.8. wsparcie dla IPv6;

2.2.17.1.9. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

2.2.17.1.10. integracja z Active Directory;

2.2.17.1.11. wsparcie dla dynamic DNS;

2.2.17.1.12. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

2.2.17.1.13. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

2.2.17.1.14. możliwość obsługi przez sześciu użytkowników jednocześnie;

2.2.17.1.15. możliwość podmontowania zdalnych wirtualnych napędów;

2.2.17.1.16. wirtualną konsolę z dostępem do myszy, klawiatury;

2.2.17.1.17. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

2.2.17.1.18. Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej

2.2.17.1.19. Przesyłanie danych telemetrycznych w czasie rzeczywistym

2.2.17.1.20. Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze

2.2.17.1.21. Automatyczna rejestracja certyfikatów (ACE)

2.2.18. Oprogramowanie do zarządzania

2.2.18.1. Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

2.2.18.1.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych

2.2.18.1.2. integracja z Active Directory

2.2.18.1.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta

2.2.18.1.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish

2.2.18.1.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

2.2.18.1.6. Szczegółowy opis wykrytych systemów oraz ich komponentów

2.2.18.1.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF

2.2.18.1.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

2.2.18.1.9. Grupowanie urządzeń w oparciu o kryteria użytkownika

2.2.18.1.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

2.2.18.1.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach

2.2.18.1.12. Szybki podgląd stanu środowiska

2.2.18.1.13. Podsumowanie stanu dla każdego urządzenia

2.2.18.1.14. Szczegółowy status urządzenia/elementu/komponentu

2.2.18.1.15. Generowanie alertów przy zmianie stanu urządzenia.

2.2.18.1.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń

2.2.18.1.17. Integracja z service desk producenta dostarczonej platformy sprzętowej

2.2.18.1.18. Możliwość przejęcia zdalnego pulpitu

2.2.18.1.19. Możliwość podmontowania wirtualnego napędu

2.2.18.1.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów

2.2.18.1.21. Możliwość importu plików MIB

2.2.18.1.22. Przesyłanie alertów „as-is” do innych konsol firm trzecich

2.2.18.1.23. Możliwość definiowania ról administratorów

2.2.18.1.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

2.2.18.1.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

2.2.18.1.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta

2.2.18.1.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

2.2.18.1.28. 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.

2.2.18.1.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

2.2.18.1.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

2.2.18.1.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

2.2.18.1.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

2.2.18.1.33. Zdalne uruchamianie diagnostyki serwera.

2.2.18.1.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

2.2.18.1.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

2.2.19. Wspierane systemy operacyjne

2.2.19.1. Canonical® Ubuntu® Server LTS

2.2.19.2. Citrix® Hypervisor®

2.2.19.3. Microsoft® Windows Server® with Hyper-V

2.2.19.4. Red Hat® Enterprise Linux

2.2.19.5. SUSE® Linux Enterprise server

2.2.19.6. VMware® ESXi®

2.2.20. Certyfikaty

2.2.20.1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

2.2.20.2. Serwer musi posiadać deklaracja CE.

2.2.20.3. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.

2.2.20.4. 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 Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.

2.2.20.5. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

2.2.21. Dokumentacja użytkownika

2.2.21.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

2.2.21.2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2.2.22. **Wsparcie techniczne i oprogramowanie** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania

2.2.22.1. Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego,

2.2.22.2. automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.

2.2.22.3. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.

2.2.22.4. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.

2.2.22.5. 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.

2.2.22.6. 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.

2.2.22.7. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :

2.2.22.7.1. Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.

2.2.22.7.2. Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.

2.2.22.7.3. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.

2.2.22.7.4. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,

2.2.22.7.5. 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.

2.2.22.7.6. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne

2.2.22.7.7. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.

2.2.22.7.8. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)

2.2.22.7.9. sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)

2.2.22.7.10. dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml

2.2.22.7.11. 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.

2.2.23. Warunki gwarancji

2.2.23.1. Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres 3 lat.

2.2.23.2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

2.2.23.3. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)

2.2.23.4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

2.2.23.5. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

2.2.23.6. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

2.2.23.7. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

2.2.23.8. 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

2.2.23.9. 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.

2.2.23.10. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2.2.23.11. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

3. Urządzenia typu zasilacz awaryjny (UPS)

3.1. Model UPS – TYP I-3 szt.

3.1.1. Minimalne wymagania techniczne dla jednostki UPS

3.1.1.1. Moc znamionowa jednostki nie mniej niż 5000W / 5000VA

3.1.1.2. Technologia Podwójnej konwersji (online)

3.1.1.3. Temperatura eksploatacji 0 - 40 °C

3.1.1.4. Wilgotność względna podczas pracy 0 - 95 %

3.1.1.5. Wysokość n.p.m. podczas pracy 0-3000 m

3.1.1.6. Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0 dBA

3.1.1.7. Rozpraszanie ciepła w trybie online 931.0BTU/godz.

3.1.1.8. Klasa ochrony IP 20

3.1.1.9. Klasa energetyczna sprzętu przeciwprzepięciowego 1260J

3.1.1.10. Możliwość montażu Tower / Rack (2U)

3.1.2. Parametry wejściowe

3.1.2.1. Nominalne napięcie wejściowe 230V

3.1.2.2. Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne)

3.1.2.3. Typ połączenia wejściowego: Połączenie poprzez zacisk 3-przewodowy (1fazowy + N + uziemienie)

3.1.2.4. Limity napięcia wejściowego 180 V - 275 V

3.1.3. Parametry wyjściowe

3.1.3.1. Napięcie wyjściowe 230V

3.1.3.2. Zniekształcenia napięcia wyjściowego ≤2%

3.1.3.3. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3 Hz

3.1.3.4. Inne napięcia wyjściowe 220, 240

3.1.3.5. Współczynnik szczytu 3: 1

3.1.3.6. Typ przebiegu sinusoida

3.1.3.7. Złącza/gniazda wyjściowe:

3.1.3.7.1. (4) IEC 320 C19

3.1.3.7.2. (6) IEC 320 C13

3.1.3.8. Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)

3.1.4. Akumulatory i czas podtrzymania

3.1.4.1. Litowo-jonowe

3.1.4.2. Czas podtrzymania:

3.1.4.2.1. 5 minut 17 sekund dla pełnego obciążenia

3.1.4.2.2. 11 minut 22 sekundy dla połowy obciążenia

3.1.4.3. Typowy czas ładowania 1,5 godziny

3.1.4.4. Oczekiwana żywotność akumulatora (lata) 5 - 10

3.1.4.5. Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów akumulatorowych

3.1.5. Komunikacja i zarządzanie

3.1.5.1. Gniazdo do montażu karty WEB/SNMP- Smart Slot x1

3.1.5.2. Porty komunikacyjne: RJ-45 Serial, Smart-Slot, USB

3.1.5.3. Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD

3.1.5.4. Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia

3.1.5.5. Awaryjny wyłącznik zasilania (EPO): Tak

3.1.6. Certyfikaty, zgodności oraz gwarancja

3.1.6.1. CE UKCA EN/IEC 62040-1 ROHS

3.1.6.2. 5 lat gwarancji, naprawy lub wymiany.

3.1.7. Oprogramowanie

3.1.7.1. Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

3.2. Model UPS – TYP II -3 szt.

3.2.1. Minimalne wymagania techniczne dla jednostki UPS

3.2.1.1. Moc znamionowa jednostki nie mniej niż 2200W / 2200VA

3.2.1.2. Technologia Podwójnej konwersji (online)

3.2.1.3. Temperatura eksploatacji 0 - 40 °C

3.2.1.4. Wilgotność względna podczas pracy 0 - 95 %

3.2.1.5. Wysokość n.p.m. podczas pracy 0-3000 m

3.2.1.6. Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0 dBA

3.2.1.7. Rozpraszanie ciepła w trybie online 325.0BTU/godz.

3.2.1.8. Klasa ochrony IP 20

3.2.1.9. Klasa energetyczna sprzętu przeciwprzepięciowego 1600J

3.2.1.10. Możliwość montażu Tower / Rack (1U)

3.2.2. Parametry wejściowe

3.2.2.1. Nominalne napięcie wejściowe 230V

3.2.2.2. Częstotliwość wejściowa 50–60 Hz (wykrywanie automatyczne)

3.2.2.3. Typ gniazda wejściowego: IEC 60320 C20

3.2.2.4. Inne napięcia wejściowe 220, 240

3.2.3. Parametry wyjściowe

3.2.3.1. Napięcie wyjściowe 230V

3.2.3.2. Zniekształcenia napięcia wyjściowego ≤2% dla 100% obciążenia linearnego

3.2.3.3. <5% dla 100% obciążenia nielinearnego

3.2.3.4. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3 Hz

3.2.3.5. Inne napięcia wyjściowe 220, 240

3.2.3.6. Współczynnik szczytu 3: 1

3.2.3.7. Typ przebiegu sinusoida

3.2.3.8. Złącza/gniazda wyjściowe

3.2.3.8.1. (2) IEC 320 C19

3.2.3.8.2. (3) IEC 320 C13

3.2.3.9. Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)

3.2.4. Akumulatory i czas podtrzymania

3.2.4.1. Litowo-jonowe

3.2.4.2. Czas podtrzymania:

3.2.4.2.1. 6 minut 38 sekund dla pełnego obciążenia

3.2.4.2.2. 13 minut 51 sekund dla połowy obciążenia

3.2.4.3. Typowy czas ładowania 4 godziny

3.2.4.4. Oczekiwana żywotność akumulatora (lata) 5 - 10

3.2.4.5. Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów akumulatorowych

3.2.5. Komunikacja i zarządzanie

3.2.5.1. Gniazdo do montażu karty WEB/SNMP- Smart Slot x1

3.2.5.2. Porty komunikacyjne: RJ-45 Serial, Smart-Slot, USB

3.2.5.3. Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD

3.2.5.4. Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia

3.2.5.5. Awaryjny wyłącznik zasilania (EPO): Tak

3.2.6. Certyfikaty, zgodności oraz gwarancja

3.2.6.1. CE EAC RCM VDE UKCA UK PSTI

3.2.6.2. 5 lat gwarancji, naprawy lub wymiany.

3.2.7. Oprogramowanie

3.2.7.1. Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

4. Urządzenia typu zasilacz awaryjny (UPS) – 12 szt.

4.1. Model UPS

4.1.1. Charakterystyka podstawowa

4.1.1.1. Technologia wykonania UPS: Line-interactive

4.1.1.2. Moc pozorna (VA): minimum 850

4.1.1.3. Moc rzeczywista (W): minimum 425

4.1.1.4. Kształt fali na wyjściu(praca na baterii): Symulowana fala sinusoidalna

4.1.1.5. Automatyczna regulacja napięcia (mechanizm AVR): Wymagany

4.1.1.6. Ochrona przed przeciążeniem: Wymagana (minimum bezpiecznik oraz wewnętrzny ogranicznik prądu)

4.1.1.7. Filtr EMI/RFI: Wymagany

4.1.1.8. Układ przeciwprzepięciowy (J): Wymagany, minimum 150

4.1.2. Charakterystyka wejścia/wyjścia

4.1.2.1. Nominalne napięcie wejściowe (V): 230+/-10%

4.1.2.2. Obsługiwany zakres napięcia wejściowego (V): minimum 165 - 290

4.1.2.3. Częstotliwość wejściowa(Hz): 50+/-5 ; 60+/-5

4.1.2.4. Wykrywanie częstotliwości wejściowej: Wymagane automatyczne

4.1.2.5. Napięcie przy pracy na baterii (V): 230+/-10%

4.1.2.6. Częstotliwość przy pracy baterii (Hz): 50+/-1% ; 60+/-1%

4.1.3. Charakterystyka gniazd

4.1.3.1. Rodzaj złącza wejściowego: Schuko

4.1.3.2. Gniazdka: FR x 3

4.1.4. Charakterystyka baterii

4.1.4.1. Typowy czas przełączenia na baterie (ms): 4 ms

4.1.4.2. Czas podtrzymania na baterii: Wymagana, czas pracy przy pełnym obciążeniu do 1 min, przy obciążeniu 200W do 5,5 min.

4.1.4.3. Ładowanie baterii: Typowy czas ładowania do 6 h

4.1.5. Zarządzanie

4.1.5.1. Sygnalizacja: Wymagane alarmy dźwiękowe oraz diody LED

4.1.5.2. Diody LED – syngalizacja: Zasilanie włączone, Tryb liniowy, Tryb baterii, Tryb obejścia, Niski poziom baterii, Przeciążenie, Usterka UPS

4.1.5.3. Alarmy dźwiękowe – sygnalizacja: Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS

4.1.5.4. Port komunikacyjny USB (HID): Wymagany

4.1.5.5. Dołączone oprogramowanie do zarządzania: Wymagane, obsługa platform Windows, Linux oraz mac

4.1.6. Cechy fizyczne

4.1.6.1. Obudowa: Tower

4.1.6.2. Konstrukcja obudowy: Plastikowa

4.1.6.3. Rozmiary (szer. x wys. x gł.) (mm): Nie większe niż 84 x 174 x 280

4.1.6.4. Waga: maksimum 4,2 kg (urządzenie bez opakowania i akcesoriów)

4.1.7. Dane środowiskowe

4.1.7.1. Temperatura robocza (°C): 0 - 40

4.1.7.2. Względna wilgotność robocza (bez kondensacji) (%): 0 - 90

4.1.7.3. Rozproszenie ciepła (BTU/hr): Nie więcej niż 34 BTU/hr

4.1.8. Certyfikaty

4.1.8.1. Pozostałe wymagane certyfikaty: CE, RoHS

4.1.9. Gwarancja

4.1.9.1. Na urządzenie: minimum 2 lata na urządzenie i baterie

5. Serwer typu NAS – 3 szt.

5.1.1. Obudowa

5.1.1.1. Desktop o wymiarach nie większych niż 170 mm x 350 mm x 250 mm (wysokość x szerokość x głębokość)

5.1.2. Pamięć RAM

5.1.2.1. Minimum 4GB pamięci SO-DIMM DDR4 ECC tego samego producenta co serwer.

5.1.3. Ilość obsługiwanych dysków

5.1.3.1. Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 18 dysków.

5.1.3.2. Minimum 2 dyski M.2 NVMe SSD 2280

5.1.4. Zainstalowane dyski

5.1.4.1. 8 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami:

5.1.4.1.1. prędkość obrotowa: minimum 7200 RPM,

5.1.4.1.2. pamięć cache: minimum 256 MB,

5.1.4.1.3. gwarancja: minimum 60 miesięcy,

5.1.4.1.4. MTBF: minimum 2 miliony.

5.1.4.2. Możliwość aktualizacji oprogramowania dysków bezpośrednio z interfejsu systemu operacyjnego serwera NAS.

5.1.5. Interfejsy sieciowe

5.1.5.1. Minimum 4 porty 1GbE RJ-45

5.1.5.2. Wsparcie dla Link Agregation.

5.1.6. Porty

5.1.6.1. Minimum 2 porty USB 3.2

5.1.7. Wskaźniki LED

5.1.7.1. Status, HDD 1-8, zasilanie, LAN 1-3

5.1.8. Obsługa RAID

5.1.8.1. Basic, JBOD, RAID 0, 1, 5, 6, 10, SHR wraz z obsługa dysków typu hot spare.

5.1.9. Funkcje RAID

5.1.9.1. Możliwość zwiększania pojemności i migracja między poziomami RAID online.

5.1.10. Szyfrowanie

5.1.10.1. Możliwość szyfrowania wybranych udziałów sieciowych.

5.1.11. Protokoły

5.1.11.1. SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)

5.1.12. Usługi

5.1.12.1. Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antywirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.

5.1.12.2. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.

5.1.13. Obsługa migawek

5.1.13.1. Liczba migawek folderu współdzielonego: minimum 1000

5.1.14. Zarządzanie dyskami

5.1.14.1. SMART, sprawdzanie złych sektorów.

5.1.15. Język GUI

5.1.15.1. Polski

5.1.16. Gwarancja i serwis

5.1.16.1. Minimum 3 lata gwarancji producenta.

5.1.17. Waga

5.1.17.1. Maksymalnie 8 kg

5.1.18. Pobór mocy

5.1.18.1. Maksymalnie 70W w trybie pracy.

5.1.19. Certyfikaty

5.1.19.1. CE

5.1.20. System plików

5.1.20.1. Dyski wewnętrzne: BTRFS

5.1.21. Szyfrowanie

5.1.21.1. Mechanizm szyfrowania sprzętowego (AES-NI)

5.1.22. Liczba wolumenów

5.1.22.1. Minimum 64

5.1.23. Liczba iSCSI Targetów

5.1.23.1. Minimum 125

5.1.24. Liczba iSCSI LUN

5.1.24.1. Minimum 250

5.1.25. Liczba kont użytkowników

5.1.25.1. Minimum 2000

5.1.26. Liczba grup

5.1.26.1. Minimum 255

5.1.27. Liczba folderów udostępnionych

5.1.27.1. Minimum 500

5.1.28. Ilość jednoczesnych połączeń

5.1.28.1. Minimum 1000

5.1.29. Zasilacz

5.1.29.1. Wewnętrzny zasilacz o mocy minimum 200W.

6. Oprogramowanie backup – 1szt.

6.1. Opis oprogramowania do wykonywania kopii zapasowych.

6.1.1. Oprogramowania do wykonywania kopii zapasowych wspiera następujące systemy operacyjne zarówno pod względem instalacji oprogramowania centralnego zarządzania jak i agentów:

6.1.1.1. Microsoft Windows 11

6.1.1.2. Microsoft Windows 10

6.1.1.3. Microsoft Windows 8/8.1

6.1.1.4. Microsoft Windows 7 SP1

6.1.1.5. Microsoft Windows Server 2022

6.1.1.6. Microsoft Windows Server 2019

6.1.1.7. Microsoft Windows Server 2016

6.1.1.8. Microsoft Windows Server 2012 o 2012 R2

6.1.1.9. Microsoft Windows Server 2008 R2 SP1

6.1.1.10. Ubuntu 20.04 LTS

6.1.2. Oprogramowania do wykonywania kopii zapasowych wspiera tworzenie kopii zapasowej wirtualnych maszyn z następujących platform wirtualizacyjnych:

6.1.2.1. Hyper-V

6.1.2.2. VMware ESXi 6.0

6.1.2.3. vCenter Server 6.0

6.1.2.4. VMware vSphere 6.0

6.1.3. Oprogramowania do wykonywania kopii zapasowych wspiera następujące przeglądarki:

6.1.3.1. Google Chrome 29 lub nowsza wersja

6.1.3.2. Mozilla Firefox 23 lub nowsza wersja

6.1.3.3. Microsoft Edge 25 lub nowsza wersja

6.1.4. Specyfikacja punktu dostępowego:

6.1.4.1. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość manualnej instalacji agentów na wskazanych stacjach roboczych czy serwerach.

6.1.4.2. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość zdalnej instalacji agentów na wskazanych stacjach roboczych czy serwerach.

6.1.4.3. Oprogramowania do wykonywania kopii zapasowych posiada konsole zarządzania umożliwiającej zarządzanie z poziomu przeglądarki.

6.1.4.4. Oprogramowania do wykonywania kopii zapasowych umożliwia tworzenie harmonogramu tworzenia kopii zapasowych komputerów, serwerów jak i wirtualnych maszyn.

6.1.4.5. Oprogramowania do wykonywania kopii zapasowych umożliwia tworzenie kopii zapasowych pełnych, przyrostowych, różnicowych jak i sektor po sektorze.

6.1.4.6. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowej wybranych plików, dysków jak i partycji.

6.1.4.7. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowej danych z systemów plików takich jak: NTFS, FAT32, FAT16, exFAT, ReFS, ext2, ext3, ext4.

6.1.4.8. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych dysków HDD, SSD, SSHD.

6.1.4.9. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych zewnętrznych nośników danych takich jak: pendrive'y, dyski przenośne, karty SD, itp.

6.1.4.10. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych udziałów sieciowych z serwerów NAS.

6.1.4.11. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych struktur RAIDowych.

6.1.4.12. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość utworzenia kopii zapasowych na urządzenie NAS.

6.1.4.13. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych bez przerywania pracy systemu operacyjnego dzięki integracji z Volume Shadow Copy Service.

6.1.4.14. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość sprawdzania poprawności wykonanej kopii zapasowej.

6.1.4.15. Oprogramowania do wykonywania kopii zapasowych posiada funkcjonalność ograniczania zajmowane miejsca przez kopie zapasowe po przez kompresje danych jak i deduplikacje.

6.1.4.16. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość dzielenia kopii zapasowej na części o określonej wielkości.

6.1.4.17. Oprogramowania do wykonywania kopii zapasowych posiada możliwość tworzenia kopii zapasowej wirtualnych maszyn bez konieczności instalacji dodatkowego oprogramowania w ramach platformy wirtualizacyjnej, ani do wirtualnych maszyn.

6.1.4.18. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość tworzenia kopii zapasowych baz danych.

6.1.4.19. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość dodawania komentarzy do poszczególnej kopii zapasowej.

6.1.4.20. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość

6.1.4.21. Oprogramowania do wykonywania kopii zapasowych oferuje możliwość przywrócenia poszczególnych plików z kopii zapasowej.

6.1.4.22. Oprogramowania do wykonywania kopii zapasowych posiada możliwość szyfrowania kopii zapasowych za pomocą hasła dostępowego.

6.1.4.23. Oprogramowania do wykonywania kopii zapasowych posiada możliwość powiadamiania osoby upoważnione o statusie przeprowadzonej kopii zapasowej.

6.1.4.24. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bez limitów na stacje robocze i serwery. Wykonawca musi dostarczyć licencje wieczystą.

6.1.4.25. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

7. Punkty dostępowe – 5 szt.

7.1. Opis punktu dostępowego.

7.1.1. Punkt dostępowy wspiera następujące standardy Wi-Fi:

7.1.1.1. 802.11a

7.1.1.2. 802.11b

7.1.1.3. 802.11g

7.1.1.4. 802.11n

7.1.1.5. 802.11ac

7.1.1.6. 802.11ax

7.1.2. Specyfikacja punktu dostępowego:

7.1.2.1. Punkt dostępowy posiada możliwość konfiguracji za pomocą aplikacji na urządzeniu mobilnych jak i wykorzystania dedykowanego kontrolera.

7.1.2.2. Punkt dostępowy posiada interfejs sieciowy RJ45 o szybkości nie mniejszej niż 2,5GbE.

7.1.2.3. Interfejs punktu dostępowego umożliwia przesyłanie zasilania w standardzie PoE+.

7.1.2.4. Obudowa punktu dostępowego posiadać możliwość montowanie urządzenia na powierzchniach płaskich takie jak ściana czy sufit.

7.1.2.5. Maksymalna oferowana szybkość transmisji anten punktu dostępowego nie może być mniejsza niż 573,5 Mb/s dla częstotliwości 2,4 GHz, 3,4 Gb/s dla 5 GHz i 4,8 Gb/s dla 6 GHz.

7.1.2.6. Anteny punktu dostępowego posiadają możliwość utworzenia sieci Wi-Fi o szerokości kanału na poziomie 160MHz dla częstotliwości 5GHz jak i 6GHz.

7.1.2.7. Punkt dostępowy posiada możliwość równoczesnego nawiązania połączenia z przynajmniej 600 urządzeniami.

7.1.2.8. Punkt dostępowy posiada technologie symultanicznej komunikacji z odbiornikami Wi-Fi w ilości przynajmniej 4 x 4 MU-MIMO dla częstotliwości 5 GHz jak i 6 GHz.

7.1.2.9. Punkt dostępowy wspiera znakowanie pakietów za pomocą protokołu 802.1Q.

7.1.2.10. Punkt dostępowy posiada funkcjonalność tworzenia przynajmniej 8 sieci Wi-Fi w ramach jednego urządzenia.

7.1.2.11. Punkt dostępowy posiada funkcjonalność stworzenia sieci gościnnej.

7.1.2.12. Punkt dostępowy posiada funkcjonalność izolacji urządzeń połączonych do sieci gościnnej od innych sieci Wi-Fi.

7.1.2.13. Specyfikacja zabezpieczeń komunikacji obejmuje WPA-PSK, WPA-Enterprise w wersjach: WPA, WPA2 jak i WPA3.

7.1.2.14. Punkt dostępowy umożliwia autentykacje użytkowników za pomocą serwera RADIUS.

7.1.2.15. Punkt dostępowy umożliwia regulacje szybkości transferu pakietów względem wskazanego odbiornika.

7.1.2.16. Punkt dostępowy posiada co najmniej certyfikaty CE, FCC, IC.

7.1.2.17. Punkt dostępowy umożliwia skonfigurowanie preferowanej częstotliwości przesyłu danych za pomocą, której ma odbywać się komunikacja z danych między odbiornikiem, a punktem dostępowym.

7.1.2.18. Punkt dostępowy umożliwia uruchomienie funkcji bezpieczeństwa zapobiegających odszyfrowaniu urządzeń za pomocą protokołu DHCP i IGMP.

7.1.2.19. Punkt dostępowy umożliwia filtrowanie dostępu do rozgłaszanej sieci Wi-Fi za pomocą adresu MAC urządzenia.

7.1.2.20. Punkt dostępowy umożliwia przesyłanie pakietów mDNS między rozgłaszanymi sieciami Wi-Fi.

7.1.2.21. Punkt dostępowy obsługuje protokół drzewa rozpinającego.

7.1.2.22. Punkt dostępowy umożliwia przesyłanie pakietów telefonii komórkowej za pomocą funkcjonalności Wi-Fi Calling.

7.1.2.23. Punkt dostępowy wspiera możliwość przesyłania ramek większych niż 1500 bajtów.

7.1.2.24. Punkt dostępowy posiada możliwość zmniejszenia zużycia konsumpcji energii elektrycznej przez odbiorniki podłączone do sieci Wi-Fi.

7.1.2.25. Punkt dostępowy umożliwia wykorzystanie kanałów DFSowych do rozpropagowanie sieci Wi-Fi.

7.1.2.26. Gwarancja producenta minimum 12 miesięcy.

8. Skaner podatności

8.1. Liczba licencji w ramach zapytania

8.1.1.1. 100 licencji – liczba urządzeń według adresów IP w infrastrukturze klienta

8.2. LICENCJA

8.2.1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum 24 miesięcy.

8.2.1.2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 24 miesięczną gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

8.2.1.3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.

8.2.1.4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

8.2.1.5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

8.3. WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA

8.3.1.1. Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.

8.3.1.2. Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System

powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.

8.3.1.3. Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

8.3.1.4. Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

8.3.1.5. Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

8.3.1.6. Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

8.3.1.7. Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

8.3.1.8. Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

8.3.1.9. Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

8.3.1.10. Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

8.3.1.11. Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).

8.3.1.12. Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

8.3.1.13. Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

8.3.1.14. Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

8.3.1.15. Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

8.3.1.16. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

8.3.1.17. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

8.3.1.18. Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.

8.3.1.19. Zgodność ze standardami HTML i CSS całego serwisu www.

8.3.1.20. Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

8.3.1.21. System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

8.3.1.22. System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

8.3.1.22.1. MODUŁ ANALIZY PODATNOŚCI

8.3.1.22.1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

8.3.1.22.1.1.1. System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM).

Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.

8.3.1.22.1.1.2. Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności "nowe", których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

8.3.1.22.1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

8.3.1.22.1.2.1. System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

8.3.1.22.1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

8.3.1.22.1.3.1. System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

8.3.1.22.2. MODUŁ MONITORINGU ZASOBÓW

8.3.1.22.2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

8.3.1.22.2.1.1. System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji.

Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

8.3.1.22.2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami

8.3.1.22.2.2.1. System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

8.3.1.22.2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

8.3.1.22.2.3.1. System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi mieć możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi

mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

8.3.1.22.2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

8.3.1.22.2.4.1. Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko “nowe” problemy i zdarzenia oraz te, których status nie został zmieniony na “rozwiązany” bądź “anulowany”. Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

8.3.1.22.2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

8.3.1.22.2.5.1. Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

8.3.1.22.2.6. Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

8.3.1.22.2.6.1. System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

8.3.1.22.2.7. Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

8.3.1.22.2.7.1. System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

8.3.1.22.3. MODUŁ ANALIZY LOGÓW

8.3.1.22.3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

8.3.1.22.3.1.1. Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać

informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

8.3.1.22.3.2. Możliwość analizy tzw. „customowych" logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

8.3.1.22.3.2.1. System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. "customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

8.3.1.22.3.3. Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

8.3.1.22.3.3.1. Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od - do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

8.3.1.22.3.4. Przegląd i analiza logów dotyczących działań użytkowników.

8.3.1.22.3.4.1. W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do

systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

8.3.1.22.3.5. Dostęp do logów historycznych.

8.3.1.22.3.5.1. System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

8.3.1.22.3.6. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

8.3.1.22.3.6.1. System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log “customowy”). Ponadto CSB musi informować użytkownika/administratora o “nowych” zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

8.3.1.22.3.7. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

8.3.1.22.3.7.1. System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla

użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

8.3.1.22.4. MODUŁ INWENTARYZACJI

8.3.1.22.4.1. Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

8.3.1.22.4.1.1. System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez “ręczne” wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

8.3.1.22.4.2. Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)

8.3.1.22.4.2.1. Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu “ręcznym” system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

8.3.1.22.4.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

8.3.1.22.4.3.1. Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

8.3.1.22.5. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

8.3.1.22.5.1. Integracja z systemem tiketowym.

8.3.1.22.5.1.1. System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

8.3.1.22.5.2. Zgłaszanie incydentu/problemu, który został namierzony przez system.

8.3.1.22.5.2.1. Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku “Zgłoś Problem”. Po wybraniu opcji zgłoszenia system powinien automatycznie

wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

8.3.1.22.5.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

8.3.1.22.5.3.1. System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

8.3.1.22.6. PANEL UŻYTKOWNIKA

8.3.1.22.6.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

8.3.1.22.6.1.1. Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

8.3.1.22.6.2. Wizualizacja statystyk zdarzeń i logów

8.3.1.22.6.2.1. Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

8.3.1.22.6.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”.

8.3.1.22.6.3.1. Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą

system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

8.3.1.22.6.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

8.3.1.22.6.4.1. Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

8.3.1.22.6.5. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów.

8.3.1.22.6.5.1. Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

8.4. Skanowanie sieci i zarządzanie podatnościami

8.4.1.1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym.

8.4.1.2. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania.

8.4.1.3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.

8.4.1.4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta

8.4.1.5. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych:

8.4.1.5.1. Microsoft Edge

8.4.1.5.2. Mozilla Firefox

8.4.1.5.3. Google Chrome

8.4.1.5.4. Safari

8.4.1.6. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania.

8.4.1.7. Oprogramowanie skanujące podatności, w postaci aplikacji instalowanej lokalnie, wspiera poniższe systemy operacyjne:

8.4.1.7.1. Windows Server 2012 R2 i nowsze

8.4.1.7.2. Ubuntu server 18.x LTS

8.4.1.8. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.

8.4.1.9. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:

8.4.1.9.1. wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.

8.4.1.9.2. wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.

8.4.1.9.3. Pozwala na konfigurację parametrów skanowania takich jak:

8.4.1.9.3.1. zakres przeszukiwanych portów,

8.4.1.9.3.2. wydajność skanowania (ilość jednoczesnych połączeń sieciowych),

8.4.1.9.3.3. liczbę jednoczesnych wątków skanowania,

8.4.1.9.3.4. możliwość wykrycia wersji systemu operacyjnego.

8.4.1.9.4. konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)

8.4.1.9.5. konfigurację wysyłania powiadomień na wskazany adres e-mail, informujących o rozpoczęciu skanowania oraz jego zakończeniu.

8.4.1.10. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.

8.4.1.11. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLS oraz XML.

8.4.1.12. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.

8.4.1.13. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:

8.4.1.13.1. określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.

8.4.1.13.2. masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.

8.4.1.13.3. konfigurację parametrów skanowania, takich jak:

8.4.1.13.3.1. zakres skanowanych portów sieciowych TCP/UDP,

8.4.1.13.3.2. parametr wydajności skanowania,

8.4.1.13.3.3. rodzaj uwierzytelniania na skanowanej stacji.

8.4.1.13.4. konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.

8.4.1.13.5. konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.

8.4.1.14. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.

8.4.1.15. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku.

8.4.1.16. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.

8.4.1.17. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:

8.4.1.17.1. określenie skanowanego celu za pomocą adresu URL lub adresu IP.

8.4.1.17.2. konfigurację parametrów skanowania takich jak:

8.4.1.17.2.1. rodzaje testowanych ataków,

8.4.1.17.2.2. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),

8.4.1.17.2.3. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).

8.4.1.17.3. konfigurację uwierzytelniania w testowanej aplikacji web.

8.4.1.17.4. konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.

8.4.1.17.5. konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.

8.4.1.18. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.

8.4.1.19. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.

8.4.1.20. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:

8.4.1.20.1. przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.

8.4.1.20.2. zapisywanie wskazanych warunków wyszukiwania jako szablony.

8.4.1.20.3. podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.

8.4.1.20.4. dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.

8.4.1.21. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.

8.4.1.22. Lista wszystkich wykrytych podatności musi umożliwiać:

8.4.1.22.1. filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (opis), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy.

8.4.1.22.2. wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.

8.4.1.22.3. eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.

8.4.1.23. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów.

8.4.1.24. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego.

8.4.1.25. Raport podsumowujący umożliwia:

8.4.1.25.1. konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,

8.4.1.25.2. wybranie grup urządzeń, które będą znajdowały się w raporcie,

8.4.1.25.3. wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,

8.4.1.25.4. personalizację danych, którymi zostanie podpisany raport.

8.4.1.26. Lista wygenerowanych raportów musi umożliwiać:

8.4.1.26.1. filtrowanie raportów ze względu na ich autora, nazwę, szablon oraz opis,

8.4.1.26.2. eksport wyniku raportu do pliku XML, DOCX, XLSX.

8.4.1.27. Rozwiązanie umożliwia zarządzanie wykrytymi podatności w co najmniej następujący sposób:

8.4.1.27.1. podgląd listy utworzonych zgłoszeń,

8.4.1.27.2. filtrowanie zgłoszeń ze względu na ich status oraz czas zamknięcia,

8.4.1.27.3. podgląd listy szablonów dla poszczególnych rodzajów skanów,

8.4.1.27.4. dodanie szablonu dla poszczególnych rodzajów skanów oraz wprowadzenie ich konfiguracji

8.5. Certyfikaty i standardy

8.5.1.1. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms

8.5.1.1.1. minimalne wymaganie:

8.5.1.1.2. minimalna liczba referencji 65

8.5.1.1.3. minimalna ocena z referencji 4,6

8.5.1.1.4. (załączyć wydruk)

8.5.1.2. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

8.5.1.2.1. minimalne wymaganie:

8.5.1.2.2. minimalna liczba referencji 17

8.5.1.2.3. minimalna ocena z referencji 4,4

8.5.1.2.4. (załączyć wydruk)

8.5.2. system musi posiadać certyfikaty:

8.5.2.1. OPSWAT (dla EDR na poziomie min. Platinium),

8.5.2.2. AVLAB +++

8.5.2.3. AV Comperative Advance +

8.5.2.4. AV-TEST (ochrona w 2023 na poziomie min.6)

8.5.2.5. producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ~~ISO 9001 oraz~~ 27001 oraz usługi związane z cyberbezpieczeństwem.

8.6. Rozszerzone wsparcie serwisowe

8.6.1.1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.

8.6.1.2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

8.6.1.2.1. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.

8.6.1.2.2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.

8.6.1.2.3. Doradztwo w zakresie konfiguracji.

8.6.1.2.4. Zdalne wsparcie techniczne.

8.6.1.2.5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.

8.6.1.2.6. Przygotowanie do zdalnej konfiguracji.

8.6.1.2.7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.

8.6.1.2.8. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.

8.6.1.2.9. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.

8.6.1.2.10. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

8.6.1.3. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

8.6.1.4. Oferent winien przedłożyć dokumenty:

8.6.1.4.1. Certyfikat 27001 autoryzowanego podmiotu serwisującego.

9. Oprogramowanie EDR (serwery i stacje robocze)

9.1. Liczba licencji w ramach zapytania

9.1.1.1. 49 licencji – urządzenia komputerowe

9.2. LICENCJA

9.2.1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum 24 miesiące.

9.2.1.2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 24 miesięczną gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

9.2.1.3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.

9.2.1.4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

9.2.1.5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

9.3. WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA

9.3.1. MODUŁ EDR/XDR

9.3.1.1. Integracja z systemem EDR/XDR.

9.3.1.1.1. System musi mieć możliwość integracji z systemami EDR/XDR przy wykorzystaniu API, tak aby umożliwiał informowanie użytkownika/administratora o pojawiających się incydentach i zdarzeniach dotyczących np. próby ataku czy wykrycia złośliwego oprogramowania na poszczególnych hostach.

9.3.1.2. Możliwość zarządzania systemem EDR z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

9.3.1.3. Brak konieczności instalacji dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy,

9.3.1.4. Rozwiązanie musi posiadać możliwość instalacji/działania na stacjach roboczych z co najmniej systemami operacyjnymi: Microsoft Windows 10, Microsoft Windows 11, MacOS 11.

9.3.1.5. Rozwiązanie musi posiadać możliwość instalacji/działania na serwerach z co najmniej następującymi systemami operacyjnymi: Microsoft® Windows Server 2012, 2016, 2019, 2022.

9.3.1.6. Rozwiązanie musi posiadać polski interfejs użytkownika.

9.3.1.7. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane agentem, ma możliwość współpracy z oprogramowaniem antywirusowym posiadanym przez Zamawiającego.

9.3.1.8. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.

9.3.1.9. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.

9.3.1.10. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.

9.3.1.11. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.

9.3.1.12. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:

9.3.1.12.1. dostęp do pliku;

9.3.1.12.2. tworzenie nowego procesu;

9.3.1.12.3. nawiązane połączenia sieciowe;

9.3.1.12.4. wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;

9.3.1.12.5. zawartość skryptów uruchamianych na monitorowanej stacji.

9.3.1.13. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.

9.3.1.14. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.

9.3.1.15. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.

9.3.1.16. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).

9.3.1.17. Przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.

9.3.1.18. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.

9.3.1.19. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.

9.3.1.20. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.

9.3.1.21. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.

9.3.1.22. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.

9.3.1.23. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.

9.3.1.24. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.

9.3.1.25. Każda detekcja zawiera co najmniej następujące informacje:

9.3.1.25.1. Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.

9.3.1.25.2. Data i czas wystąpienia podejrzanych zdarzeń.

9.3.1.25.3. Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.

9.3.1.25.4. Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.

9.3.1.25.5. Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.

9.3.1.25.6. Poziom ryzyka, określający istotność danej detekcji.

9.3.1.25.7. Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).

9.3.1.26. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).

9.3.1.27. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).

9.3.1.28. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.

9.3.1.29. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.

9.3.1.30. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.

9.3.1.31. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.

9.3.1.32. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.

9.3.1.33. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.

9.3.1.34. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.

9.3.1.35. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.

9.3.1.36. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.

9.3.1.37. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.

9.3.1.38. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.

9.3.1.39. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.

9.3.1.40. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.

9.3.1.41. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.

9.3.1.42. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

9.3.1.43. Podgląd informacji, alertów i zdarzeń występujących w środowisku IT

9.3.1.43.1. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

9.3.1.44. Bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego)

9.3.1.44.1. Poza integracją i prezentacją incydentów/zdarzeń występujących na poszczególnych hostach w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

9.4. Ochrona punktów końcowych urządzeń komputerowych

9.4.1.1. Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

9.4.1.2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

9.4.1.3. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

9.4.1.3.1. Microsoft Windows 10

9.4.1.3.2. Microsoft Windows 11

9.4.1.3.3. macOS 11 "Big Sur"

9.4.1.3.4. macOS 10.15 "Catalina"

9.4.1.3.5. macOS 10.14 "Mojave"

9.4.1.3.6. MacOS 10.15 “Catalina”

9.4.1.4. Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

9.4.1.4.1. Microsoft Windows Server 2012

9.4.1.4.2. Microsoft Windows Server 2016

9.4.1.4.3. Microsoft Windows Server 2019

9.4.1.4.4. Microsoft Windows Server 2022

9.4.1.5. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

9.4.1.5.1. Microsoft Internet Explorer

9.4.1.5.2. Microsoft Edge

9.4.1.5.3. Mozilla Firefox

9.4.1.5.4. Google Chrome

9.4.1.5.5. Safari

9.4.1.6. Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

9.4.1.7. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

9.4.1.8. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

9.4.2. Opis technologii

9.4.2.1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.

9.4.2.2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.

9.4.2.3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)

9.4.2.4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.

9.4.2.5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.

9.4.2.6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.

9.4.2.7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.

9.4.2.8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.

9.4.2.9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.

9.4.2.10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.

9.4.2.11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.

9.4.2.12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.

9.4.2.13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.

9.4.2.14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

9.4.2.15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.

9.4.2.16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.

9.4.2.17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.

9.4.2.18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.

9.4.2.19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.

9.4.2.20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

9.4.2.21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.

9.4.2.22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.

9.4.2.23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.

9.4.2.24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.

9.4.2.25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.

9.4.2.26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.

9.4.2.27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym

9.4.2.28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

9.4.2.29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

9.4.2.30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.

9.4.2.31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".

9.4.2.32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.

9.4.2.33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.

9.4.2.34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.

9.4.2.35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.

9.4.2.36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.

9.4.2.37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.

9.4.2.38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.

9.4.2.39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

9.4.2.40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

9.4.2.41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.

9.4.2.42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.

9.4.2.43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.

9.4.2.44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.

9.4.2.45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.

9.4.2.46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.

9.4.2.47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.

9.4.2.48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.

9.4.2.49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.

9.4.2.50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

9.4.2.51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.

9.4.2.52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.

9.4.2.53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny

dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.

9.4.2.54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.

9.4.2.55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna" czyści zawartość schowka systemowego.

9.4.2.56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.

9.4.2.57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

9.4.2.58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.

9.4.2.59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).

9.4.2.60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.

9.4.2.61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.

9.4.2.62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.

9.4.2.63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

9.4.2.64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.

9.4.2.65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.

9.4.2.66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.

9.4.2.67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.

9.4.2.68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

9.4.2.69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.

9.4.2.70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

9.4.2.71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

9.4.2.72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.

9.4.2.73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.

9.4.2.74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.

9.4.2.75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.

9.4.2.76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.

9.4.2.77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.

9.4.2.78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.

9.4.2.79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.

9.4.2.80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

9.4.2.81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.

9.4.2.82. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker

9.4.2.83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.

9.4.2.84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.

9.4.2.85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.

9.4.2.86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.

9.4.2.87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.

9.4.2.88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)

9.4.2.89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.

9.4.2.90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.

9.4.2.91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.

9.4.2.92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.

9.4.2.93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

9.4.2.94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.

9.4.2.95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

9.4.2.96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

9.4.2.97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.

9.4.2.98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.

9.4.2.99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji

9.4.2.100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.

9.4.2.101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

9.4.2.102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.

9.4.2.103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN

9.4.2.104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika,

zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)

9.4.2.105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.

9.4.2.106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).

9.4.2.107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

9.4.3. Centralna administracja

9.4.3.1. Portal zarządzający jest dostępny w języku polskim.

9.4.3.2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.

9.4.3.3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.

9.4.3.4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.

9.4.3.5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.

9.4.3.6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.

9.4.3.7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.

9.4.3.8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.

9.4.3.9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.

9.4.3.10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.

9.4.3.11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.

9.4.3.12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.

9.4.3.13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.

9.4.3.14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.

9.4.3.15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.

9.4.3.16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.

9.4.3.17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.

9.4.3.18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.

9.4.3.19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.

9.4.3.20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

9.4.3.21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

9.4.3.22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

9.4.3.23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.

9.4.3.24. Profile mogą być przypisane do pojedynczych hostów lub do grup.

9.4.3.25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.

9.4.3.26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.

9.4.3.27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.

9.4.3.28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.

9.4.3.29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.

9.4.3.30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.

9.4.3.31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.

9.4.3.32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.

9.4.3.33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.

9.4.3.34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.

9.4.3.35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.

9.4.3.36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

9.5. Certyfikaty i standardy

9.5.1.1. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms

9.5.1.1.1. minimalne wymaganie:

9.5.1.1.1.1. minimalna liczba referencji 65

9.5.1.1.1.2. minimalna ocena z referencji 4,6

9.5.1.1.2. (załączyć wydruk)

9.5.1.2. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

9.5.1.2.1. minimalne wymaganie:

9.5.1.2.1.1. minimalna liczba referencji 17

9.5.1.2.1.2. minimalna ocena z referencji 4,4

9.5.1.2.2. (załączyć wydruk)

9.5.2. system musi posiadać certyfikaty:

9.5.2.1. OPSWAT (dla EDR na poziomie min. Platinium),

9.5.2.2. AVLAB +++

9.5.2.3. AV Comperative Advance +

9.5.2.4. AV-TEST (ochrona w 2023 na poziomie min.6)

9.5.2.5. producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO-27001 oraz usługi związane z cyberbezpieczeństwem.

9.6. Rozszerzone wsparcie serwisowe

9.6.1.1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia

zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.

9.6.1.2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

9.6.1.2.1. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.

9.6.1.2.2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.

9.6.1.2.3. Doradztwo w zakresie konfiguracji.

9.6.1.2.4. Zdalne wsparcie techniczne.

9.6.1.2.5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.

9.6.1.2.6. Przygotowanie do zdalnej konfiguracji.

9.6.1.2.7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.

9.6.1.2.8. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.

9.6.1.2.9. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.

9.6.1.2.10. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

9.6.1.3. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

9.6.2. Oferent winien przedłożyć dokumenty:

9.6.2.1. Certyfikat ~~ISO~~ 27001 autoryzowanego podmiotu serwisującego.

10. Oprogramowanie do inwentaryzacji i monitorowania sieci IT

10.1. SYSTEM DO ZARZĄDZANIA INFRASTRUKTURĄ IT

10.1.1. Architektura / budowa

10.1.1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 49 Klientów jednocześnie.

10.1.1.2. Architektura / budowa:

10.1.1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.

10.1.1.2.1.1. Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.3.

10.1.1.2.1.2. Serwer i klient posiadają certyfikaty SSL (4096 bitowe).

10.1.1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).

10.1.1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.

10.1.1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.

10.1.1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.

10.1.1.3. Konfiguracja Architektury:

10.1.1.3.1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.

10.1.1.3.2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.

10.1.1.3.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.

10.1.1.3.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.

10.1.1.3.5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi.

10.1.1.3.6. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.

10.1.1.3.7. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.

10.1.1.3.8. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

10.1.1.3.9. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

10.1.1.3.10. Klient musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

10.1.1.3.11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.

10.1.1.3.12. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

10.1.1.3.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów.

10.1.1.4. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.

10.1.1.4.1. Automaty powinny realizować co najmniej:

10.1.1.4.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych.

10.1.1.4.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.

10.1.2. Wymagania systemowe

10.1.2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).

10.1.2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

10.1.2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2

10.1.2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.

10.1.2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.

10.1.2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).

10.1.2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

10.1.3. Interfejsy

10.1.3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

10.1.3.1.1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

10.1.3.1.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.

10.1.3.1.3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.

10.1.3.2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.

10.1.3.3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

10.1.3.4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

10.1.3.5. System zapewnia integrację z modelem LLM.

10.1.4. Funkcjonalności systemu zarządzania infrastrukturą IT

10.1.4.1. Funkcjonalność Klienta

10.1.4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).

10.1.4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość

10.1.4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.

10.1.4.2. Funkcjonalność konsoli administracyjnej.

10.1.4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje językową angielską.

10.1.4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

10.1.4.2.3. Konsola administracyjna musi posiadać minimum 140 dashboardów – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

10.1.4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór widżetu.

10.1.4.2.5. Dashboard prezentujący parametry sieci zawiera widżety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.

10.1.4.2.5.1. Lista monitorowanych usług: AIM/ICQ, Back Orifice, Bagle.B, Bagle.h, BGMP, BGP, BitTorrent, Blaster, Blizzard's Battle.net, Call of Duty, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, Doom, Emule, FTP (connection control), FTP (data port), FTPS

(TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), GameSpy Arcade, Gnutella, Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, Jedi Knight: Jedi Academy, Kazza, Kerberos, Killing Floor, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NFS, Niektóre gry firmy Blizzard, Nintendo Wi-Fi Connection, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Radio internetowe, Rbot/Spybot, RDP, rsyns, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP, SMB, SMTP,SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, Sub7, Symantec System Center Klient, TACACS, TeamViewier, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo,! Messenger.

10.1.4.2.6. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.

10.1.4.2.7. Dashboard prezentujący informacje o bezpieczeństwie zawiera widżety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez BitLockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez Klienta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych, nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cal, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie CPU, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

10.1.4.2.8. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

10.1.4.2.9. Dane na widżetach muszą być aktualizowane automatycznie.

10.1.4.2.10. Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany odpowiadające mu widżety (np. w obszarze zarządzania

komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)

10.1.4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.

10.1.4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).

10.1.4.2.12.1. System musi oferować możliwość dodawania własnych pól zarówno w głównym widoku, jak i w obszarze zarządzania użytkownikami. Te definiowalne pola powinny być w pełni funkcjonalne i umożliwiać:

10.1.4.2.12.1.1. Dodawanie nazwy kolumny, określenie jej typu oraz możliwość ograniczenia liczby znaków, które można wprowadzić.

10.1.4.2.12.1.2. Wśród obsługiwanych typów pól znajdują się: tekst, liczba całkowita, liczba, data, data i czas, combobox.

10.1.4.2.12.2. W ramach personalizacji widoku, system powinien oferować możliwość zastosowania filtrów dostosowujących zawartość danego widoku. Filtry te powinny:

10.1.4.2.12.2.1. Bazować na kolumnach dostępnych w danym widoku.

10.1.4.2.12.2.2. Umożliwiać selekcję operacji filtrujących takich jak: równość, nierówność, większość, mniejszość, obecność lub brak wartości.

10.1.4.2.12.2.3. Pozwalać na łączenie filtrów przy użyciu logicznych operatorów „AND” (i), „OR” (lub), „NOT AND” (i nie), „NOT OR” (lub nie).

10.1.4.2.12.2.4. Być zapamiętywane przez system dla konkretnej sesji użytkownika i pozostawać aktywne po ponownym zalogowaniu.

10.1.4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator Klienta, strukturę organizacyjną, stan Klienta (włączony/wyłączony),

nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.

10.1.4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

10.1.4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

10.1.4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

10.1.4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

10.1.4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

10.1.4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).

10.1.4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)

10.1.4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

10.1.4.3. Funkcjonalność panelu pracownika

10.1.4.3.1. Automatyczne uruchamianie panelu oraz autoryzacja w momencie zalogowania użytkownika do systemu operacyjnego.

10.1.4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.

10.1.4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.

10.1.4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji.

10.1.4.3.5. Sekcje informacyjne panelu pracownika

10.1.4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – Nazwa użytkownika, Imię, Nazwisko, E-mail, Firma, Dział, Stanowisko, Struktura org., Kraj, Województwo, Miasto, Ulica, Kod pocztowy, Telefon, Telefon komórkowy, Opis, WWW, GG, Skype, Adres, Biuro, Skrytka pocztowa

10.1.4.3.6. Dashboard

10.1.4.3.6.1. Mój komputer – wykorzystanie RAM, Dysk, CPU.

10.1.4.3.6.2. Produktywność - czas zalogowania, aktywność, produktywność.

10.1.4.3.6.3. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.

10.1.4.3.6.4. Skróty – definiowane przez administratora skróty do adresów URL, z możliwością edycji tytułu, opisu, koloru tekstu i tła

10.1.4.3.7. Sprzęt

10.1.4.3.7.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

10.1.4.3.7.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

10.1.4.3.7.3. Urządzenia przypisane do pracownika (nr seryjny, typ, IP).

10.1.4.3.8. Oprogramowanie

10.1.4.3.8.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie w okresie ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).

10.1.4.3.9. Informacja o czasie pracy

10.1.4.3.9.1. Lista otwartych sesji pracownika lub grupy pracowników (data zalogowania, nazwa komputera, IP, rodzaj połączenia (LAN, NAT, VPN), czas zalogowania).

10.1.4.3.9.2. Lista ostatnich sesji użytkownika lub grupy użytkowników (początek, koniec, czas trwania sesji, nazwa komputera, IP)

10.1.4.3.9.3. Lista używanego oprogramowania (nazwa aplikacji, wersja, producent, data ostatniego uruchomienia, użycie aplikacji w ostatnich 3, 6, 12 miesiącach).

10.1.4.3.9.4. Aktywność użytkownika lub użytkowników w aplikacjach (aplikacja, kategoria aplikacji, łączny czas korzystania, czas korzystania aktywnego, czas korzystania pasywnego).

10.1.4.3.9.5. Aktywność użytkownika lub użytkowników w Internecie (adres URL, informacja o stronie www –kategoria strony czy strona jest produktywna, łączny czas korzystania, czas aktywności, czas pasywności).

10.1.4.3.9.6. Wydruki – lista wydrukowanych dokumentów – data, godzina, nazwa drukarki, nazwa dokumentu

10.1.4.4. Zarządzanie licencjami

10.1.4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).

10.1.4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.

10.1.4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.

10.1.4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania", które definiują 3 kategorie oprogramowania: „oprogramowanie zalecane" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.

10.1.4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.

10.1.4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).

10.1.4.4.7. System musi umożliwiać kategoryzację uruchamianych procesów.

10.1.4.4.7.1. Umożliwia zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.

10.1.4.4.7.2. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.

10.1.4.4.7.3. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.

10.1.4.4.7.4. Niezależność od zewnętrznych dostawców bazy wzorców procesów.

10.1.4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).

10.1.4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam, gdzie jest to tylko technicznie możliwe.

10.1.4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.

10.1.4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.

10.1.4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.

10.1.4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.

10.1.4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).

10.1.4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.

10.1.4.4.16. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.

10.1.4.4.17. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).

10.1.4.4.18. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).

10.1.4.4.19. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.

10.1.4.4.20. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.

10.1.4.4.21. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.

10.1.4.4.22. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.

10.1.4.4.23. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.

10.1.4.5. Wzorce aplikacji i pakietów

10.1.4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.

10.1.4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.

10.1.4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.

10.1.4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.

10.1.4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.

10.1.4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

10.1.4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam, gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

10.1.4.6. Inwentaryzacja sprzętu komputerowego

10.1.4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).

10.1.4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.

10.1.4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).

10.1.4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.

10.1.4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.

10.1.4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).

10.1.4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

10.1.4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.

10.1.4.6.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.

10.1.4.6.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).

10.1.4.6.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.

10.1.4.6.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.

10.1.4.6.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)

10.1.4.6.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu.

10.1.4.6.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).

10.1.4.6.15.1. System musi umożliwiać definiowanie typów serwisów

10.1.4.6.15.2. System musi umożliwiać definiowanie wartości serwisu

10.1.4.6.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji

10.1.4.6.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.

10.1.4.6.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).

10.1.4.7. Inwentaryzacja urządzeń podłączanych do komputera.

10.1.4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)

10.1.4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.

10.1.4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).

10.1.4.8. Inwentaryzacja urządzeń sieciowych.

10.1.4.8.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.

10.1.4.8.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.

10.1.4.8.3. System musi zbierać informacje o jakości połączenia:

10.1.4.8.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach:

10.1.4.8.4.1. Średni czas odpowiedzi.

10.1.4.8.4.2. Minimalny czas odpowiedzi.

10.1.4.8.4.3. Maksymalny czas odpowiedzi.

10.1.4.8.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

10.1.4.8.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta, a w przypadku, gdy takiego Klienta nie posiadają powinien umożliwić zdalną instalację Klienta.

10.1.4.8.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci

10.1.4.8.6.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.

10.1.4.8.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.

10.1.4.8.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.

10.1.4.8.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

10.1.4.9. Inwentaryzacja sprzętu.

10.1.4.9.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.

10.1.4.9.1.1. System musi umożliwiać bazy typów urządzeń, o dowolne typy.

10.1.4.9.2. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.

10.1.4.9.3. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.

10.1.4.9.4. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.

10.1.4.9.5. System musi mieć możliwość przypominania o upływającym terminie gwarancji.

10.1.4.9.6. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.

10.1.4.9.7. System udostępnia informację o wartości wprowadzonego sprzętu.

10.1.4.9.8. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.

10.1.4.9.9. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.

10.1.4.9.10. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

10.1.4.10. Ochrona danych (DLP)

10.1.4.10.1. System automatycznie tworzy listę podłączanych do komputerów urządzeń USB.

10.1.4.10.2. System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)

10.1.4.10.3. System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.

10.1.4.10.4. System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.

10.1.4.10.5. System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB).

10.1.4.10.6. System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły.

10.1.4.11. Zdalna administracja komputerami

10.1.4.11.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

10.1.4.11.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

10.1.4.11.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia

dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

10.1.4.11.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

10.1.4.11.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.

10.1.4.11.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów

10.1.4.11.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

10.1.4.11.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

10.1.4.11.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

10.1.4.11.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

10.1.4.11.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

10.1.4.11.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie)

komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

10.1.4.11.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

10.1.4.11.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).

10.1.4.11.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).

10.1.4.11.3.1. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.

10.1.4.11.3.2. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.

10.1.4.11.3.3. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

10.1.4.12. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

10.1.4.13. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

10.1.4.14. Zdalne Zarządzanie Zaporą (Firewall)

10.1.4.14.1. System powinien umożliwiać monitorowanie stanu zapory w czasie rzeczywistym, zapewniając aktualne informacje o jej działaniu.

10.1.4.14.2. System powinien zapewniać zdalne sterowanie zaporą na dowolnych komputerach, co obejmuje:

10.1.4.14.2.1. Definiowanie i zarządzanie złożonymi zasadami zapory z centralnego panelu administracyjnego.

10.1.4.14.3. System powinien umożliwiać szybkie identyfikowanie i reagowanie na potencjalne zagrożenia, zwiększając bezpieczeństwo sieci.

10.1.4.14.4. System powinien oferować kontrolę ruchu sieciowego, umożliwiając zarządzanie dostępem do zasobów sieciowych.

10.1.4.15. Automatyzacja

10.1.4.15.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.

10.1.4.15.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.

10.1.4.15.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.

10.1.4.15.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).

10.1.4.15.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,

10.1.4.16. Zarządzanie magazynem IT

10.1.4.16.1. System musi umożliwiać obsługę magazynu IT.

10.1.4.16.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

10.1.4.16.3. System musi umożliwiać obsługę dokumentów PZ, RW, WZ, MM+, MM-, LI.

10.1.4.16.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło, pierwsze wyszło).

10.1.4.16.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.

10.1.4.16.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.

10.1.4.16.7. System musi umożliwiać automatyczne łączenie wygenerowanych dokumentów z zasobami systemu, takimi jak osoby, urządzenia.

10.1.4.16.8. System musi zapewniać możliwość przeglądu wszystkich wygenerowanych dokumentów.

10.1.4.17. Repozytorium

10.1.4.17.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.

10.1.4.17.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

10.1.4.17.3. Repozytorium musi umożliwić definiowanie kontenerów na dokumenty.

10.1.4.18. Kody kreskowe

10.1.4.18.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.

10.1.4.18.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.

10.1.4.18.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.

10.1.4.18.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.

10.1.4.18.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.

10.1.4.18.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix,

EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.

10.1.4.18.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.

10.1.4.18.8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.

10.1.4.19. Wysyłanie wiadomości

10.1.4.19.1. Komunikator

10.1.4.19.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.

10.1.4.19.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora.

10.1.4.19.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.

10.1.4.19.1.4. System musi przechowywać historię konwersacji.

10.1.4.19.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.

10.1.4.19.2. Wiadomość Jednorazowa:

10.1.4.19.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.

10.1.4.19.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.

10.1.4.19.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.

10.1.4.19.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników.

10.1.4.19.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.

10.1.4.19.3. Wiadomości Cykliczne:

10.1.4.19.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.

10.1.4.19.3.2. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.

10.1.4.19.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.

10.1.4.19.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.

10.1.4.19.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.

10.1.4.19.4. System szkolenia pracowników za pomocą wiadomości.

10.1.4.19.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.

10.1.4.19.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa", „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa", „Postępowanie w przypadku naruszenia tajemnicy", „Udostępnienie informacji stanowiących tajemnicę".

10.1.4.19.4.3. Formatowanie treści musi być zgodne z HTML.

10.1.4.19.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).

10.1.4.19.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.

10.1.4.19.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

10.1.4.19.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

10.1.4.19.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.

10.1.4.19.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).

10.1.4.20. System musi posiadać możliwość eksportu / importu treści.

10.1.4.21. Monitorowanie drukarek sieciowych i wydruków

10.1.4.21.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).

10.1.4.21.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.

10.1.4.21.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany definiowalny przez administratora systemu, cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.

10.1.4.21.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.

10.1.4.21.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.

10.1.4.21.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.

10.1.4.21.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

10.1.4.22. Monitorowanie stron www

10.1.4.22.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.

10.1.4.22.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.

10.1.4.22.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).

10.1.4.22.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.

10.1.4.22.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści stron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.

10.1.4.22.5.1. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.

10.1.4.23. Monitorowanie serwerów WWW

10.1.4.23.1. System musi umożliwiać monitorowanie wybranych serwerów www.

10.1.4.23.1.1. System musi przedstawiać informację o działaniu wybranych serwerów oraz ich aktywności.

10.1.4.23.1.2. System musi posiadać możliwość weryfikacji treści (tekstu) dostępnego na monitorowanej stronie.

10.1.4.23.1.3. System w sposób graficzny musi przedstawiać działanie serwerów WWW wraz z wyszczególnieniem informacji dla każdego wybranego serwera (status, bieżący czas odpowiedzi, średni czas odpowiedzi za ostatnie 12 miesięcy, aktywność za ostatnie 3, 6, 12 miesięcy).

10.1.4.24. Monitorowanie dziennika zdarzeń

10.1.4.24.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.

10.1.4.24.2. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.

10.1.4.24.3. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.

10.1.4.25. System musi umożliwiać monitorowanie komunikatów Syslog.

10.1.4.26. Monitorowanie pracy komputerów

10.1.4.26.1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.

10.1.4.26.2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.

10.1.4.26.3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie

10.1.4.26.4. Monitorowanie sesji zdalnych połączeń

10.1.4.26.4.1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.

10.1.4.26.4.2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera, z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.

10.1.4.27. Monitorowanie sensorów

10.1.4.27.1. System musi umożliwić integrację z systemem monitoringu warunków środowiskowych poprzez odczyt wartości z wykorzystaniem SNMP.

10.1.4.27.2. Czujniki muszą być grupowane wg typu oraz lokalizacji.

10.1.4.27.3. System musi prezentować położenie czujników na mapie wbudowanej w system.

10.1.4.27.4. System musi umożliwić odczyt informacji z czujników temperatury, wilgotności oraz odczytywać zmiany stanu czujników zalania oraz otwarcia drzwi.

10.1.4.27.5. System musi przechowywać odczytane dane w bazie danych przez zadany okres.

10.1.4.27.6. System musi umożliwić wysyłanie alertów poprzez email, sms oraz prezentować informację w konsoli o przekroczeniu monitorowanych parametrów.

10.1.4.27.7. System musi umożliwić graficzną prezentację danych zebranych z monitorowanych czujników.

10.1.4.28. Repozytorium CMDB

10.1.4.28.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:

10.1.4.28.1.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.

10.1.4.28.1.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.

10.1.4.28.1.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.

10.1.4.28.1.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.

10.1.4.28.1.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.

10.1.4.28.1.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.

10.1.4.28.1.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.

10.1.4.28.1.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.

10.1.4.28.1.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.

10.1.4.28.1.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.

10.1.4.28.1.11. Typy licencji - lista typów licencji.

10.1.4.28.1.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.

10.1.4.28.1.13. Typy urządzeń - lista typów urządzeń.

10.1.4.28.1.14. Urządzenia - lista urządzeń podzielonych wg typu.

10.1.4.28.1.15. Producenci / Dostawcy - lista producentów i dostawców.

10.1.4.28.1.16. Pamięć masowa - zestawienie dysków twardych z komputerów.

10.1.4.28.1.17. Porty sieciowe - lista monitorowanych portów sieciowych.

10.1.4.28.1.18. Usługi sieciowe - lista monitorowanych usług sieciowych.

10.1.4.28.1.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.

10.1.4.28.1.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.

10.1.4.28.1.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.

10.1.4.28.1.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.

10.1.4.28.1.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.

10.1.4.28.1.24. Serwery - lista zinwentaryzowanych serwerów.

10.1.4.28.1.25. Usługi - zestawienie usług działających na komputerach.

10.1.4.28.1.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.

10.1.4.28.1.27. Pamięć masowa USB - lista urządzeń pamięci masowej USB.

10.1.4.28.1.28. Administratorzy - lista administratorów systemu,

10.1.4.28.1.29. Użytkownicy / pracownicy - lista pracowników.

10.1.4.28.1.30. Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.

10.1.4.28.1.31. Serwisy WWW - lista monitorowanych serwisów WWW.

10.1.4.29. Worktime manager

10.1.4.29.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.

10.1.4.29.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.

10.1.4.29.2.1. System musi umożliwiać prezentację szczegółowych informacji o przypisanej grupie bezpośrednio w panelu pracownika na pulpicie przełożonego, który jest przypisany do tej grupy.

10.1.4.29.3. Dane muszą być prezentowane w formie interaktywnych widżetów oraz w formie danych analitycznych.

10.1.4.29.4. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.

10.1.4.29.4.1. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.

10.1.4.29.4.2. Informacje prezentowane w panelu: informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera,

informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.

10.1.4.29.5. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.

10.1.4.29.6. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.

10.1.4.29.7. System musi posiadać widgety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.

10.1.4.30. Raportowanie i eksport danych

10.1.4.30.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.

10.1.4.30.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).

10.1.4.30.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.

10.1.4.30.4. Generowanie raportu musi odbywać się po stronie serwera a nie klienta.

10.1.4.30.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).

10.1.4.30.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt) oraz Stimulsoft.

10.1.4.30.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.

10.1.4.30.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).

10.1.4.30.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących obszarów funkcjonalnych.

10.1.4.30.9.1. Raporty z zakresu komputerów

10.1.4.30.9.1.1. Komputery – Karta graficzna – Procesor

10.1.4.30.9.1.2. Komputery – Serwery wg systemu operacyjnego

10.1.4.30.9.1.3. Komputery wg procesora – Skrócony

10.1.4.30.9.1.4. Komputery wg procesora – Wszystkie

10.1.4.30.9.1.5. Komputery wg producenta – Skrócony

10.1.4.30.9.1.6. Komputery wg producenta – Wszyscy

10.1.4.30.9.1.7. Komputery wg struktur organizacyjnych – Skrócony

10.1.4.30.9.1.8. Komputery wg struktury organizacyjnej – Wszystkie

10.1.4.30.9.1.9. Komputery wg systemów operacyjnych – Skrócony

10.1.4.30.9.1.10. Komputery wg systemów operacyjnych – Wszystkie

10.1.4.30.9.1.11. Komputery wg typu – Desktop

10.1.4.30.9.1.12. Komputery wg typu – Hyper-V

10.1.4.30.9.1.13. Komputery wg typu – Mobile

10.1.4.30.9.1.14. Komputery wg typu – Nieokreślone

10.1.4.30.9.1.15. Komputery wg typu – Server

10.1.4.30.9.1.16. Komputery wg typu – Virtual Machine

10.1.4.30.9.1.17. Komputery wg typu – VMWare

10.1.4.30.9.1.18. Komputery wg typu – Wszystkie typy

10.1.4.30.9.1.19. Zestawienie komputerów wg typu – Skrócony

10.1.4.30.9.1.20. Komputery online

10.1.4.30.9.1.21. Komputery niezautoryzowane

10.1.4.30.9.1.22. Komputery offline

10.1.4.30.9.1.23. Komputery online

10.1.4.30.9.1.24. Komputery w magazynie

10.1.4.30.9.1.25. Komputery w naprawie

10.1.4.30.9.1.26. Komputery wszystkie

10.1.4.30.9.1.27. Komputery wycofane

10.1.4.30.9.1.28. Komputery zablokowane

10.1.4.30.9.1.29. Komputery zautoryzowane

10.1.4.30.9.1.30. Komputery zlikwidowane

10.1.4.30.9.1.31. Komputery z Intel Anti-Theft

10.1.4.30.9.1.32. Komputery z Intel VPro

10.1.4.30.9.2. Raporty z zakresu urządzeń

10.1.4.30.9.2.1. Urządzenia – Notatki

10.1.4.30.9.2.2. Urządzenia – USB – Dodane

10.1.4.30.9.2.3. Urządzenia – USB – Wykryte

10.1.4.30.9.2.4. Urządzenia – USB – Wszystkie

10.1.4.30.9.2.5. Urządzenia – USB – Biała lista

10.1.4.30.9.2.6. Urządzenia – Serwis

10.1.4.30.9.2.7. Urządzenia – Inwentaryzacja – Kody kreskowe

10.1.4.30.9.2.8. Urządzenia – Inwentaryzacja

10.1.4.30.9.2.9. Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji

10.1.4.30.9.2.10. Urządzenia – Utrzymanie

10.1.4.30.9.2.11. Urządzenia

10.1.4.30.9.3. Raporty z zakresu sieci

10.1.4.30.9.3.1. Sieć – Wykryte

10.1.4.30.9.3.2. Sieć – Historia

10.1.4.30.9.3.3. Sieć – Ostanie skanowanie

10.1.4.30.9.4. Raporty z zakresu oprogramowania

10.1.4.30.9.4.1. Oprogramowanie – Systemy operacyjne – Wszystkie

10.1.4.30.9.4.2. Oprogramowanie – Systemy operacyjne – Instalacje OEM

10.1.4.30.9.4.3. Oprogramowanie – Systemy operacyjne – Szczegóły

10.1.4.30.9.4.4. Oprogramowanie – Systemy operacyjne – Historia audytów

10.1.4.30.9.4.5. Oprogramowanie – Aplikacje – Wszystkie

10.1.4.30.9.4.6. Oprogramowanie – Aplikacje – Monitorowane

10.1.4.30.9.4.7. Oprogramowanie – Aplikacje – Szczegóły

10.1.4.30.9.4.8. Oprogramowanie – Aplikacje – Historia audytów

10.1.4.30.9.4.9. Oprogramowanie – Pakiety – Wszystkie

10.1.4.30.9.4.10. Oprogramowanie – Pakiety – Szczegóły

10.1.4.30.9.4.11. Oprogramowanie – Pakiety – Historia audytów

10.1.4.30.9.4.12. Oprogramowanie – Bazy danych – Wszystkie

10.1.4.30.9.4.13. Oprogramowanie – Bazy danych – Express

10.1.4.30.9.4.14. Oprogramowanie – Bazy danych – Pozostałe

10.1.4.30.9.4.15. Oprogramowanie – Bazy danych – per Core

10.1.4.30.9.4.16. Oprogramowanie – Rejestry – Razem

10.1.4.30.9.4.17. Oprogramowanie – Rejestry – Szczegóły

10.1.4.30.9.4.18. Oprogramowanie – Rejestry – Ostatnio zainstalowane

10.1.4.30.9.4.19. Oprogramowanie – Klucze produktu

10.1.4.30.9.4.20. Oprogramowanie – Wykorzystanie – Użycie – Wszystkie

10.1.4.30.9.4.21. Oprogramowanie – Wykorzystanie – Oszczędności

10.1.4.30.9.4.22. Oprogramowanie – Wykorzystanie – CAL

10.1.4.30.9.4.23. Oprogramowanie – Wykorzystanie – CAL WEB

10.1.4.30.9.4.24. Oprogramowanie – Monitorowanie – Uruchomienia

10.1.4.30.9.4.25. Oprogramowanie – Monitorowanie – Aktywność ogółem

10.1.4.30.9.5. Raporty z zakresu osób

10.1.4.30.9.5.1. Osoby – Protokół standardowy

10.1.4.30.9.5.2. Osoby – Protokół rozszerzony

10.1.4.30.9.6. Raporty z zakresu plików i multimediów

10.1.4.30.9.6.1. Pliki i multimedia – Archiwa

10.1.4.30.9.6.2. Pliki i multimedia – Audio

10.1.4.30.9.6.3. Pliki i multimedia – Erotyka

10.1.4.30.9.6.4. Pliki i multimedia – Grafika

10.1.4.30.9.6.5. Pliki i multimedia – Wideo

10.1.4.30.9.6.6. Pliki i multimedia – Wykonywalne

10.1.4.30.9.6.7. Pliki i multimedia – Zmiany plików

10.1.4.30.9.7. Raporty z zakresu magazynu

10.1.4.30.9.7.1. Magazyn – Dokumenty

10.1.4.30.9.7.2. Magazyn – Stany

10.1.4.30.9.7.3. Magazyn – Materiały

10.1.4.30.9.7.4. Magazyn

10.1.4.30.9.8. Raporty z zakresu finansów

10.1.4.30.9.8.1. Finanse – Urządzenia

10.1.4.30.9.8.2. Finanse – Licencje

10.1.4.30.9.8.3. Finanse – Wydruki wg drukarki

10.1.4.30.9.8.4. Finanse – Wydruki wg sterownika

10.1.4.30.9.8.5. Finanse – Wydruki użytkownicy

10.1.4.30.9.8.6. Finanse – Magazyn

10.1.4.30.9.9. Raporty z zakresu serwera wiadomości

10.1.4.30.9.9.1. Serwer wiadomości – Komunikator – Historia

10.1.4.30.9.9.2. Wiadomość cykliczna – wg wiadomości

10.1.4.30.9.9.3. Serwer wiadomości – Komunikator – Rozmowy

10.1.4.30.9.9.4. Serwer wiadomości – Wiadomości wysłane – wg komputera

10.1.4.30.9.9.5. Serwer wiadomości – Wiadomości wysłane – wg odbiorcy

10.1.4.30.9.9.6. Serwer wiadomości – Wiadomości wysłane – wg wiadomości

10.1.4.30.9.9.7. Serwer wiadomości – Wiadomości wysłane – wg wysyłającego

10.1.4.30.9.9.8. Serwer wiadomości – Wiadomości – Aktywne cykle

10.1.4.30.9.10. Raporty z zakresu serwera monitorującego

10.1.4.30.9.10.1. Serwer monitorujący – Logowanie Klientów

10.1.4.30.9.10.2. Serwer monitorujący – eServer

10.1.4.30.9.10.3. Serwer monitorujący – Alerty systemowe

10.1.4.30.9.10.4. Serwer monitorujący – Historia logowań

10.1.4.30.9.10.5. Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe

10.1.4.30.9.10.6. Serwer monitorujący – Dzienniki zdarzeń – Dzienniki

10.1.4.30.9.10.7. Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP

10.1.4.30.9.10.8. Serwer monitorujący – Transfer sieciowy – Procesy

10.1.4.30.9.10.9. Serwer monitorujący – Drukowanie

10.1.4.30.9.10.10. Serwer monitorujący – Drukowanie – Razem

10.1.4.30.9.10.11. Serwer monitorujący – Drukowanie – Razem SNMP

10.1.4.30.9.10.12. Serwer monitorujący – Drukowanie – Prognoza

10.1.4.30.9.10.13. Serwer monitorujący – Usługi – Wszystkie

10.1.4.30.9.10.14. Serwer monitorujący – Usługi – Szczegóły

10.1.4.30.9.10.15. Serwer monitorujący – Harmonogram zadań

10.1.4.30.9.10.16. Serwer monitorujący – Sesje VNC

10.1.4.30.9.10.17. Serwer monitorujący – Intel AMT

10.1.4.30.9.10.18. Serwer monitorujący – Poczta wychodząca

10.1.4.30.9.10.19. Serwer monitorujący – Strony www – Odwiedzone

10.1.4.30.9.10.20. Serwer monitorujący – Strony www – Aktywność ogółem

10.1.4.30.9.10.21. Serwer monitorujący – USB

10.1.4.30.9.10.22. Serwer monitorujący – Wydajność – CPU

10.1.4.30.9.10.23. Serwer monitorujący – Wydajność – Dysk

10.1.4.30.9.10.24. Serwer monitorujący – Wydajność – Dysk (razem)

10.1.4.30.9.10.25. Serwer monitorujący – Wydajność – Pamięć

10.1.4.30.9.10.26. Serwer monitorujący – Wydajność – Procesy

10.1.4.30.9.10.27. Serwer monitorujący – Wydajność – Sieć

10.1.4.30.9.11. Raporty z zakresu serwera zadań

10.1.4.30.9.11.1. Serwer zadań – Logi

10.1.4.30.9.11.2. Serwer zadań – Zadania cykliczne

10.1.4.30.9.11.3. Raporty z zakresu serwera automatyzacji

10.1.4.30.9.11.4. Serwer automatyzacji – Automaty

10.1.4.30.9.11.5. Serwer automatyzacji – Logi

10.1.4.30.9.12. Raporty z zakresu raportów

10.1.4.30.9.12.1. Raporty – Harmonogram

10.1.4.30.9.12.2. Raporty – Harmonogram – Historia

10.1.4.30.9.13. Raporty z zakresu repozytorium

10.1.4.30.9.13.1. Repozytorium – Dokumenty

10.1.4.30.9.13.2. Repozytorium – e-Learning

10.1.4.30.9.13.3. Repozytorium – Kategorie aplikacji

10.1.4.30.9.13.4. Repozytorium – Kategorie plików

10.1.4.30.9.13.5. Repozytorium – Kategorie procesów

10.1.4.30.9.13.6. Repozytorium – Kategorie www

10.1.4.30.9.13.7. Repozytorium – Producenci Dostawcy

10.1.4.30.9.13.8. Repozytorium – Typy licencji

10.1.4.30.9.14. Raporty z zakresu ustawień

10.1.4.30.9.14.1. Ustawienia – Administratorzy – Wszystkie

10.1.4.30.9.14.2. Ustawienia – Dane firmy

10.1.4.30.9.14.3. Ustawienia – Struktura organizacyjna

10.1.4.30.9.14.4. Ustawienia – Budżet

10.1.4.30.9.14.5. Ustawienia – Sieci

10.1.4.30.10. System musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

10.1.4.30.11. Wynikiem wykonania harmonogramu jest raport w formacie pdf.

10.1.4.31. System musi zapewnić interfejs API.

10.1.4.31.1. System musi udostępniać możliwości komunikacji z systemem za pomocą REST API.

10.1.4.31.2. Komunikacja z REST API musi odbywać się w sposób szyfrowany min. Protokołem TLS 1.3 i chroniony kluczem alfanumerycznym.

10.1.4.31.3. System musi zapewniać możliwości modyfikacji i dostosowania klucza zabezpieczeń REST API i pozwalać na ustanowienie klucza o długości co najmniej 32 znaków.

10.1.4.31.4. System musi pozwalać na tworzeni requestów obsługujących parametry w formacie JSON.

10.1.4.31.5. W ramach REST API konieczne musi być możliwość pobierania danych ze wszystkich tabel systemu, zawierających dane merytoryczne.

10.1.4.31.6. System musi przyjmować requesty pozwalające na umieszczanie danych w systemie za pomocą REST API.

10.1.4.31.7. System musi dopuszczać komunikację złożoną, za pomocą sekwencji requestwów REST API.

10.1.4.31.8. System musi pozwalać na automatyczną komunikację za pomocą REST API z innymi systemami z wykorzystaniem składni API systemu.

10.1.4.32. Powiadomienia

10.1.4.32.1. System musi umożliwiać generowanie powiadomienia.

10.1.4.32.1.1. Powiadomienia muszą być w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.

10.1.4.32.1.2. Powiadomienie musi umożliwiać automatyczne wywalanie zadania zdefiniowanego w konsoli systemu. Dostępne polecenia CMD, Windows PowerShell (minimum 70 predefiniowanych, możliwość generowania własnych, integracja z LLM).

10.1.4.32.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców

10.1.4.32.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.

10.1.4.32.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych

10.1.4.32.4.1. Powiadomienia z zakresu oprogramowania

10.1.4.32.4.1.1. Odinstalowano oprogramowanie

10.1.4.32.4.1.2. Wykryto niezgodność ze schematem oprogramowania

10.1.4.32.4.1.3. Wykryto nowe oprogramowanie

10.1.4.32.4.2. Powiadomienia z zakresu sieci

10.1.4.32.4.2.1. Monitorowana usługa sieciowa przestała odpowiadać

10.1.4.32.4.2.2. Monitorowane urządzenia z problemami

10.1.4.32.4.2.3. Monitorowane urządzenie jest offline

10.1.4.32.4.2.4. Problem ze stroną WWW

10.1.4.32.4.2.5. Serwis WWW nie odpowiada

10.1.4.32.4.2.6. Serwis WWW odpowiada niewłaściwym komunikatem

10.1.4.32.4.2.7. Średni czas odpowiedzi usługi przekroczył wartość X ms

10.1.4.32.4.2.8. Transfer sieciowy na komputerze przekroczył X MB / Y min

10.1.4.32.4.2.9. W sieci pojawiły się duplikaty adresów IP

10.1.4.32.4.2.10. W sieci pojawiły się duplikaty adresów MAC

10.1.4.32.4.2.11. Wykryto dużą ilość danych wysyłanych przez dany port w switch'u

10.1.4.32.4.2.12. Wykryto nowe urządzenie

10.1.4.32.4.2.13. Wykryto urządzenie z odblokowanym portem X

10.1.4.32.4.2.14. Wykryto urządzenie z usługą X

10.1.4.32.4.2.15. Wykryto zmianę adres IP komputera

10.1.4.32.4.2.16. Wykryto zmianę statusów portów w switch'u

10.1.4.32.4.3. Powiadomienia z zakresu sprzętu

10.1.4.32.4.3.1. Interfejs sieciowy wyłączony

10.1.4.32.4.3.2. Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości

10.1.4.32.4.3.3. Podłączono urządzenie USB

10.1.4.32.4.3.4. Wykryto zmianę w sprzęcie (WMI)

10.1.4.32.4.3.5. Powiadomienia z zakresu systemu

10.1.4.32.4.3.6. Mało miejsca na dysku C

10.1.4.32.4.3.7. Pojawił się błąd w dzienniku zdarzeń Windows

10.1.4.32.4.3.8. Wykryto problem z usługą systemu Windows

10.1.4.32.4.3.9. Wykryto zmianę nazwy komputera

10.1.4.32.4.3.10. Zmieniono informację o systemie

10.1.4.32.4.4. Powiadomienia z zakresu użytkownika

10.1.4.32.4.4.1. Użytkownik odwiedził stronę WWW z wybranej kategorii

10.1.4.32.4.4.2. Użytkownik przekroczył limit wydrukowanych stron

10.1.4.32.4.4.3. Użytkownik przekroczył transfer sieciowy X MB / Y min

10.1.4.33. Bezpieczeństwo

10.1.4.33.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.

10.1.4.33.2. Uwierzytelnianie do systemu musi być realizowane:

10.1.4.33.2.1. z wykorzystaniem imiennego konta użytkownika i hasła,

10.1.4.33.2.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,

10.1.4.33.2.3. za pośrednictwem uwierzytelniania poprzez Active Directory,

10.1.4.33.2.4. za pośrednictwem uwierzytelniania poprzez CAS,

10.1.4.33.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.

10.1.4.33.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).

10.1.4.33.5. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).

10.1.4.33.5.1. Uwierzytelnianie z wykorzystaniem obrazu wideo.

10.1.4.33.5.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika.

10.1.4.33.5.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.

10.1.4.33.6. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.

10.1.4.33.6.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.

10.1.4.33.7. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:

10.1.4.33.7.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.

10.1.4.33.7.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.

10.1.4.33.8. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

10.1.4.33.9. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.

10.1.4.33.9.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.

10.1.4.33.10. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.

10.1.4.33.11. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

10.1.4.33.12. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

10.1.4.33.13. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.

10.1.4.33.14. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).

10.1.4.33.15. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.

10.1.4.33.16. System musi zapewniać:

10.1.4.33.16.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.

10.1.4.33.16.2. Przechowywanie logów systemowych.

10.1.4.33.16.3. Przechowywanie logów bezpieczeństwa.

10.1.4.33.16.4. Przechowywanie logów aktywności użytkowników i administratorów.

10.1.4.33.16.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.

10.1.4.33.16.6. Możliwość eksportu logów.

10.1.4.33.16.7. Definiowanie maksymalnego czasu przechowywania plików log.

10.1.4.33.16.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

10.1.4.33.16.9. Definiowanie ścieżki do kopii zapasowej

10.1.4.33.16.10. Definiowanie ścieżki do importu danych

10.1.4.33.16.11. Definiowanie ścieżki do zapisu raportów

10.1.4.33.16.12. Definiowanie serwera do importu danych

10.1.5. Wsparcie i pomoc

10.1.5.1.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinariów w języku polskim.

10.1.5.1.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

10.1.5.1.3. Pomoc techniczna

10.1.5.1.3.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

10.1.5.1.3.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

10.1.5.1.3.3. Czas trwania usługi SLA wynosi 24 miesięcy od dnia zakupu.

10.1.5.1.3.4. Usługi Utrzymania Oprogramowania obejmują:

10.1.5.1.3.4.1. asystę techniczną,

10.1.5.1.3.4.2. świadczenie usług SLA, w ramach, których realizowana jest:

10.1.5.1.3.4.2.1. obsługa zgłoszeń w zakresie:

10.1.5.1.3.4.2.1.1. reakcja na zgłoszenia błędów w określonym czasie reakcji;

10.1.5.1.3.4.2.1.2. dokonywanie analizy przyczyn błędów;

10.1.5.1.3.4.2.1.3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;

10.1.5.1.3.4.2.1.4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;

10.1.5.1.3.4.2.1.5. usuwania błędów w czasie naprawy;

10.1.5.1.3.4.2.1.6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;

10.1.5.1.3.5. zapewnienia dostępności Oprogramowania.