FORMULARZ PARAMETRÓW WYMAGANYCH

1. Firewall – 2 sztuki

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

- System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
- 16 portami Gigabit Ethernet RJ-45.
- 8 gniazdami SFP 1 Gbps.
- 2 gniazdami SFP+ 10 Gbps.
- System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

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

minimum 1 Gbps.

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

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

Polityki, Firewall

- Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
- Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
- Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
- Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
  - Amazon Web Services (AWS).
  - Microsoft Azure.
  - Cisco ACI.
  - Google Cloud Platform (GCP).
  - OpenStack.
  - VMware NSX.
  - Kubernetes.

Połączenia VPN

FORMULARZ PARAMETRÓW WYMAGANYCH

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

FORMULARZ PARAMETRÓW WYMAGANYCH

- System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

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

Ochrona przed atakami

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

Kontrola aplikacji

- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

FORMULARZ PARAMETRÓW WYMAGANYCH

- Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
- Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
- System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

- System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
  - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
  - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
  - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
- System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
- Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
- Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
- System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w

wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
- System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
- Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
- Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

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

Certyfikaty
Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:
- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje
Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie
Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Instalacja
- fizyczny montaż klastra urządzeń UTM w miejscu wskazanym przez Zamawiającego
- konfiguracja klastra HA z dostarczanych urządzeń
- konfiguracja interfejsów sieciowych
- konfiguracja routingu pomiędzy podsieciami
- konfiguracja polityk ruchu – polityk firewall w uzgodnieniu z Zamawiającym
- uruchomienie mechanizmów bezpieczeństwa IPS, antywirus itp. oraz logowania ruchu dla

polityk ruchu
- konfiguracja translacji adresów NAT/PAT w uzgodnieniu z Zamawiającym
- konfiguracja bezpiecznych tuneli VPN w uzgodnieniu z Zamawiającym
- instruktarz stanowiskowy min. 3h z zakresu przeprowadzonego wdrożenia

2. Przełączniki zarządzane– 2 sztuki

Minimalne parametry techniczne

1. **Porty przełącznika**: minimum 20x 10/100/1000Base-T RJ45 wpierające PoE/PoE+, minimum 4x COMBO (10/100/1000Base-T RJ45 wspierające PoE/PoE+ lub 100/1000Base-X SFP) oraz minimum 4x 1/10GBase-X SFP+
2. **Port konsolowy:** RJ45 (RS-232)
3. **Port zarządzania:** RJ45 (10/100Base-T RJ45)
4. **Port USB:** minimum 1 port co najmniej w standardzie 2.0
5. **Szybkość przełączania:** minimum128Gb/s
6. **Przepustowość:** minimum95Mp/s (dla pakietów 64Kb)
7. **Bufor pakietów:** minimum1,5MB
8. **Ramki Jumbo:** minimum10k
9. **Tablica adresów MAC:** minimum16k
10. **Adresy MAC – Multicast:** minimum 4k
11. **Tablica ACL:** minimum 1k
12. **Tablica VLAN:** minimum 4094
13. **Tablica routingu:** minimum 1k dla IPv4 z możliwością wykorzystania IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.
14. **Taktowanie procesora:** minimum 800MHz
15. **Pamięć Flash:** minimum 128MB
16. **Pamięć RAM:** minimum 512MB
17. **Temperatura pracy:** zakres minimum 0°C - 50°C
18. **Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)
19. **Obsługa technologii PoE:** IEEE 802.3 af (15,4W), IEEE 802.3at (30W)
20. **Budżet mocy PoE:** minimum 370W
21. **Zasilanie:** zabudowany zasilacz 230V AC
22. **Pobór mocy:** maksymalnie 471W
23. **Zabezpieczenie przeciwprzepięciowe:** minimum 4kV
24. **Wymiary:** maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 320mm
25. **Certyfikaty bezpieczeństwa**: CE, RoHS
26. **Algorytmpracy:** Store and Forward
27. **Obsługa VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
28. **DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
29. **Drzewo rozpinające:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Loopback Detection, Fast Link
30. **Protekcja ringowa:** ITU-T G.8032 – recovery time < 50ms
31. **Protokoły routingu:** Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect, GRE Tunnel
32. **Agregacja linków:** IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance

FORMULARZ PARAMETRÓW WYMAGANYCH

33. **Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
34. **Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM, IGMP authentication

3.System Ochrony Poczty

Wymagania ogólne systemu

1. System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową.
2. System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https
3. System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów.
4. Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji.
5. System musi być dostępny w postaci pliku ISO pozwalającym na instalację na serwerze fizycznym, jak też w wersji na maszyny wirtualne ze wsparciem dla następujących środowisk: VMWare, Citrix, MS Hyper-V.
6. Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs.
7. System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak:
    a. Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej
    b. Wersję systemu i bieżącą datę
    c. Informacje o typie aktualnie używanego procesora
    d. Informacje o stanie skanerów antywirusowych
    e. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości
    f. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń
    g. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe
8. System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta.
9. Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy.
10. System musi mieć możliwość obsługi certyfikatów SSL.
11. System musi mieć możliwość importu certyfikatów.
12. System musi mieć możliwość obsługi TLS.
13. System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane DKIM
14. System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż SPF, DMARC, ARC.
15. System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze amazona, jak i na żądanie, a także możliwość importu takiej konfiguracji.
16. System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla

logów dotyczących inferface'u oraz zmian w systemie
17. System musi wspierać SNMP v2c oraz v3
18. System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów).
19. Aktualizacja systemu musi odbywać się poprzez konsolę webową, oraz nie może mieć wpływu na działanie samego systemu (tj. żadna wiadomość mailowa nie zostanie utracona). W przypadku aktualizacji systemów działających w klastrze, musi istnieć możliwość uruchomienia tych procesów oddzielnie (np. w przypadku gdyby aktualizacja okazała się wadliwa)

Moduł antyspamowy

1. System musi posiadać wbudowany silnik antyspamowy.
2. System musi mieć umożliwiać korzystanie z zewnętrznych baz RBL, dowolnie definiowanych przez administratora.
3. System musi mieć możliwość tworzenia przez administratora białej listy adresów IP nadawcy, pomijanych podczas filtracji RBL.
4. System musi mieć możliwość wyłączania filtracji RBL dla poszczególnych domen podpiętych do rozwiązania.
5. System musi mieć możliwość sprawdzenia poprawności odbiorcy danej wiadomości, w trybie co najmniej: dynamicznym (weryfikacja na serwerze docelowym), LDAP, listę dozwolonych odbiorców oraz poprzez wyrażenia regularne.
6. System musi być wspierany samouczącą się bazą danych Bayes'a.
7. System musi obsługiwać Passive OS Fingerprinting oraz mechanizm Penpals i analizę Botnetów.
8. System musi posiadać konfigurowalną szarą listę, z możliwością jej włączenia i wyłączenia
9. System musi pozwalać na zdefiniowanie języków, w których to muszą być napisane wiadomości, by pomyślnie przeszły weryfikację
10. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach email oraz nazwach domen. Listy powinny być traktowane globalnie, per domena i osobno dla każdego użytkownika.
11. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach IP serwerów pocztowych nadawcy.
12. System musi mieć możliwość indywidualnego ustalania wysokości progu filtrowania wiadomości przez moduł antyspamowy dla domen jak i również dla określonych aliasów pocztowych.
13. System musi mieć możliwość rozczytywania skróconych wersji URLi
14. System musi mieć możliwość dodawania konfigurowalnych stopek do maili wychodzących, które potwierdzą że zostały one przefiltrowane przez tenże system

Moduł antywirusowy

1. System musi zawierać dwa niezależnie działające silniki antywirusowe zewnętrznego dostawcy.
2. System musi mieć możliwość całkowitego wyłączenia silnika antywirusowego.
3. System musi samoczynnie aktualizować bazę danych dla wbudowanego silnika antywirusowego. Baza musi być aktualizowana minimum, co godzinę.

Moduł kontroli treści

1. System musi umożliwiać blokowanie wybranych przez administratora rozszerzeń i nazw plików.

FORMULARZ PARAMETRÓW WYMAGANYCH

2. System musi umożliwiać blokowanie co najmniej następujących rozszerzeń plików:
   ade, adp, bat, chm, cmd, com, cpl, dll, doc, exe, hta, ins, isp, jar, js, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh
3. System musi umożliwiać blokowanie co najmniej następujących typów MIME:
   application/ecmascript, application/javascript, application/x-javascript, application/x-msdos-program, application/x-msdownload, text/ecmascript, text/javascript
4. Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum.
5. System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów.
6. System musi umożliwiać tworzenie własnych reguł filtracji.
7. System musi umożliwiać kontrolę treści opartej na słowniku lub wyrażeniu regularnym (przykładowo blokowanie wiadomości z numerami kard kredytowych, numerami PESEL czy też innymi danymi określanymi jako wrażliwe).
8. Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących.
9. System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń:
   a. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu
   b. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu.
   c. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo.

Moduł powiadamiania użytkowników

1. System musi posiadać moduł powiadamiający adresata bądź odbiorcę wiadomości o podjętych przez system akcjach.
2. System musi powiadamiać o zablokowanych wiadomościach w tym wiadomościach zablokowanych przez moduł antyspamowy, antywirusowy czy moduł kontroli treści.
3. Wiadomości powinny być edytowalne i wysyłane do odbiorcy lub/i nadawcy.

Kwarantanna

1. System musi posiadać mechanizm kwarantanny.
2. System musi zawierać wbudowaną wyszukiwarkę.
3. System musi generować raporty kwarantanny
   a. Raporty kwarantanny powinny być generowane automatycznie lub na żądanie
   b. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta)
   c. Raporty powinny być generowane dla użytkowników systemu pocztowego.
   d. W przypadku współpracy z serwerami pocztowymi Microsoft Exchange, raport powinien być generowany dla użytkownika tylko raz, uwzględniając jego wszystkie aliasy.
4. System musi umożliwić dostęp do kwarantanny poprzez interfejs przeglądarki internetowej dla każdego użytkownika indywidualnie z możliwością dopasowania odpowiednich uprawnień.
5. System musi umożliwić uwierzytelnianie użytkownika za pośrednictwem wewnętrznej bazy, LDAP, w oparciu o bazę kont na docelowym serwerze pocztowym (POP3, IMAP),

lub bazy SQL.

Pozostałe funkcjonalności

1. System musi mieć możliwość tworzenie wielu administratorów o zróżnicowanym poziomie uprawnień.
2. System musi mieć możliwość tworzenia grup domen przyporządkowanych odpowiednim administratorom.
3. System musi posiadać funkcję kontroli ilości przetwarzanych wiadomości dla ruchu przychodzącego i wychodzącego.
4. System musi umożliwiać wyświetlanie statystyk dotyczących aktualnego użycia licencji (liczby unikalnych kont mailowych, przez które przechodzą wiadomości).
5. System musi umożliwiać manualne ustawienie równocześnie pracujących procesów SMTP w celu optymalizacji wydajności rozwiązania względem platformy, na której jest zainstalowane.
6. System musi posiadać moduł kontroli jakości, który pozwoli zdefiniować ograniczenia odnoszące się do co najmniej:
    a. ilości maili, które mogą zostać wysłane z określonej jednostce czasu
    b. zbiorczego rozmiaru maili, które mogą zostać wysłane w określonej jednostce czasu
7. System musi mieć możliwość ujednolicenia aliasów emailowych
8. System powinien mieć możliwość konfiguracji raportów generowanych użytkownikom tak, aby mogły być generowane na żądanie (z opcją wyłączenia tej opcji przez administratora).

Wymagania licencyjne

1. System musi pozwalać na filtrowanie poczty dla minimum 100 użytkowników
2. Okres ważności licencji 3 lata
3. Okres dostępu do wsparcia oraz aktualizacji 3 lata

Zamawiający wymaga dostawy usługi wdrożenia w minimalnym zakresie

1. Instalacja oprogramowania na wskazanym serwerze.
2. Konfiguracja inicjalizująca.
3. Aktywacja platformy.
4. Konfiguracja rozwiązania według wytycznych obejmująca m.in.:
    a. ustawienia sieciowe,
    b. synchronizację czasu,
    c. uwierzytelnianie użytkowników,
    d. połączenie z serwerem poczty elektronicznej,
    e. wstępną konfigurację polityk poczty przychodzącej i wychodzącej,
    f. reguły filtrowania treści, w tym ustawienia antywirusowe oraz załączniki,
    g. silnik antyspamowy, w tym RBL'e, baza Bayes'a, Penpals,
    h. pomoc w konfiguracji reguł poczty wychodzącej,
    i. dodanie wyjątków,
    j. konfigurację kwarantanny,
    k. personalizację serwera.

Zamawiający wymaga przeprowadzenia szkolenia administracyjnego dla 2ch osób

FORMULARZ PARAMETRÓW WYMAGANYCH

4.System EDR

Wymagania systemu

System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.
Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.
Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

- Microsoft Windows 7 z dodatkiem SP1
- Microsoft Windows 8.1 (32-bit i 64-bit)
- Microsoft Windows 10
- Microsoft Windows 11
- MacOS 11 “Big Sur”
- MacOS 10.15 “Catalina”
- MacOS 10.14 “Mojave”

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

- Microsoft® Windows Server 2008 R2
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2016
- Microsoft® Windows Server 2019
- Microsoft® Windows Server 2022

Wspierane przeglądarki internetowe:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta,

w celu wykrywania niebezpiecznych zdarzeń.

6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
    - dostęp do pliku;
    - tworzenie nowego procesu;
    - nawiązane połączenia sieciowe;
    - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
    - zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Maksymalna ilość wysyłanych danych przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 25MB na 24 godziny.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
11. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
12. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
13. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
14. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
15. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
16. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
17. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
18. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
19. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
20. Każda detekcja zawiera co najmniej następujące informacje:
    - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
    - Data i czas wystąpienia podejrzanych zdarzeń.
    - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
    - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
    - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
    - Poziom ryzyka, określający istotność danej detekcji.
    - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C,

FORMULARZ PARAMETRÓW WYMAGANYCH

nieuprawnione wykonanie skryptu).

21. 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).
22. 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).
23. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
24. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
25. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
26. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
27. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
28. Rozwiązanie monitoruje aplikacje uruchomione na stacjach roboczych i serwerach i oznacza aplikacje zidentyfikowane jako szkodliwe lub potencjalnie niebezpieczne dla użytkownika.
29. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
30. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
31. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
32. 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.
33. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
34. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
35. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
36. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
37. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
38. 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.
39. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
40. 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.
41. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
42. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w

celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

43. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
44. Dostarczona licencja musi pozwalać na ochronę 65 systemów Windows oraz 4 systemów Windows Server
45. Dostarczona licencja być ważna na okres 3 lat oraz musi zapewniać w tym czasie dostęp do wsparcia oraz aktualizacji.
46. Wraz z dostawą rozwiązania wykonawca musi zapewnić usługę wdrożenia w minimalnym zakresie:
    1. Przygotowanie paczek instalacyjnych.
    2. Instalacja limitowanej liczby agentów.
    3. Ustawienie krytyczności danych komputerów.
    4. Ustawienie odpowiedniej reguły odpowiedzi automatycznej.
    5. Konfiguracja raportowania i alertowania.
    6. Utworzenie kont administracyjnych.
    7. Test poprawności działania systemu.
47. Zamawiający wymaga przeprowadzenia szkolenia administracyjnego dla 2ch osób

5. System do zarządzania

Zarządzanie zasobami

1. Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne

- Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
- Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
- Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
- Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
- Odwzorowanie struktury organizacji w oparciu o Active Directory
- Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
- Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci
- Mapowanie atrybutów obiektów AD do obiektów oferowanego systemu
- Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
- Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
- Utworzenie własnych typów elementów wyposażenia
- Łączenie elementów wyposażenia w zestawy
- Przypisywanie zasobu do wielu zestawów

FORMULARZ PARAMETRÓW WYMAGANYCH

- Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
- Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
- Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
- Przypisywanie sprzętu do konkretnych osób
- Przypisywanie sprzętu do wybranej firmy
- Automatyczne wyznaczanie 'Głównego użytkownika' komputera
- Wiązanie wielu rekordów wyposażenia z użytkownikiem
- Przypisywanie sprzętu do dowolnej lokalizacji
- Definiowanie własnych, dowolnych atrybutów sprzętu
- Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
- Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
- Określanie loga firmy oraz użycia go na wydrukach
- Grupowa zmiana domeny/grupy roboczej zasobu

2. Informacje o sprzęcie

- Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
- Wykrywanie komputerów typu All-In-One
- Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
- Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
- Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
- Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
- Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
- Odczyt informacji o module TPM

FORMULARZ PARAMETRÓW WYMAGANYCH

- Odczyt D3Dscore z WinSAT
- Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe:
- Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
- Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
- Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
- Automatyczne tworzenie zestawów: Komputer + Monitor
- Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
- Automatyczne utworzenie zestawów: host + maszyny wirtualne
- Automatyczne wykrywanie czy komputer jest maszyną wirtualną
- Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
- Określanie informacji o wykorzystywanej wirtualizacji
- Podgląd zestawów, do których należy zasób
- Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
- Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
- Definiowanie szczegółowych informacji finansowych
- Obsługa walut w danych finansowych
- Definiowanie bazy dostawców sprzętu i oprogramowania
- Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
- Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
- Agent odczytuje identyfikator SID komputera
- Określanie adresu interfejsu webowego urządzenia sieciowego
- Określanie typu gwarancji dla zasobu
- Określenie wpływu biznesowego wybranego zasobu
- Tworzenie własnych typów gwarancji

FORMULARZ PARAMETRÓW WYMAGANYCH

- Określanie ikony dla typów zasobów

Raporty zasobów

- Raport dodanych załączników
- Automatyczne tworzenie historii zmian sprzętu
- Raport zbiorczy historii zmian w sprzęcie
- Ewidencja zdarzeń serwisowych
- Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
- Informacja na temat pojemności dysków twardych oraz wolnego miejsca
- Wydruk\dodanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu
- Wydruk\dodanie jako załącznik protokołu przekazania dla całego zestawu
- Kreator szablonów wydruków WYSIWYG
- Definiowanie dedykowanych profili protokołów
- Zapisywanie protokołów podczas generowania jako załącznik do zasobu
- Wydruk\dodanie jako załącznik Karty informacyjnej dla elementu wyposażenia
- Wydruk lub zapisanie do pliku raportów ze szczegółami sprzętu
- Porównywarka wyników skanowania sprzętu
- Dzienniki zdarzeń systemu Windows
- Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu

Funkcje dodatkowe

- Zdalne wykonywanie skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych
- Wykonywanie zadań dla wszystkich komputerów (uwzględnia komputery, które zostaną dodane w przyszłości)
- Edytor skryptów (batch) z funkcją kolorowania składni Wykorzystywanie predefiniowanych skryptów (batch) Import informacji o wyposażeniu z pliku CSV
- Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
- Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)

FORMULARZ PARAMETRÓW WYMAGANYCH

- Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
- Obsługa kodów QR
- Archiwum zasobów
- Przeniesienie utylizowanego wyposażenia do archiwum
- Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
- Zarządzanie sprzętem przez aplikacje mobilną (Android, Windows Phone) Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej Grupowa zmiana atrybutów
- Personalizacja statusów zasobów

Zarządzanie oprogramowaniem

Licencje

- Inwentaryzacja licencji
- Automatyczne tworzenie licencji na podstawie kluczy produktów
- Import licencji z pliku tekstowego
- Automatyczne generowanie historii zmian w licencji
- Określanie statusu licencji
- Utworzenie własnych atrybutów licencji
- Tworzenie notatek oraz załączników w dowolnym formacie do licencji
- Tworzenie licencji z poziomu rozliczenia audytu legalności
- Tworzenie licencji z poziomu raportu kluczy licencji
- Tworzenie zestawów licencji
- Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
- Zmiana typu licencji dla wybranej grupy
- Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
- Przypisywanie licencji do komputera
- Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)

FORMULARZ PARAMETRÓW WYMAGANYCH

- Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
- Definiowanie licencji przeznaczonych do przyszłego zakupu
- Definiowanie kluczy seryjnych i przypisywanie do licencji
- Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
- Określenie wpływu biznesowego wybranej licencji

Skanowanie oprogramowania

- Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
- Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
- Śledzenie zmian w stanie zainstalowanego oprogramowania
- Zdalny skan komputerów (bieżący lub okresowy)
- Zmiana priorytetu skanowania oprogramowania
- Skan komputerów niepodłączonych do sieci
- Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
- Przekazywanie konfiguracji wzorcowej dla skanera offline
- Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
- Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
- Określanie masek plików dla publikacji elektronicznych (e-book)
- Skan plików skompresowanych
- Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
- Wbudowane profile skanowania (np. profil wzorcowy)
- Definicja własnych ustawień skanowania
- Porównywanie wyników skanowania oprogramowania
- Wykrywanie plików multimedialnych
- Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
- Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
- Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
- Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
- Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
- Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)

Audyt legalności

- Rozliczanie pakietów aplikacji
- Rozliczanie systemów operacyjnych
- Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji
- Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów

licencji.
- Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
- Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
- Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
- Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji

Funkcje

- Mechanizm informujący o nowej bazie wzorców oprogramowania
- Definiowanie własnych wzorców oprogramowania
- Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
- Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
- Wykrywanie kluczy/identyfikatorów programów
- W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
- Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania

- Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
- Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
- Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
- "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
- Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
- Zdalne dezinstalacja oprogramowania
- Utworzenie harmonogramu dezinstalacji oprogramowania
- Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
- Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej Raport zainstalowanych aktualizacji systemu Windows

Kontrola wykorzystania sprzętu i oprogramowania

Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne

- Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
- Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
- Określanie firmy do której należy użytkownik
- Określanie przełożonego dla użytkownika
- Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy).

FORMULARZ PARAMETRÓW WYMAGANYCH

- Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
- Zarządzanie stanowiskami użytkowników
- Przeniesienie rekordu użytkownika do archiwum
- Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
- Odczytywanie informacji o użytkownikach z Active Directory
- Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
- Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
- Podgląd zdjęcia przypisanego do użytkownika
- Przypisywanie do użytkownika załączników (pliki)
- Przypisywanie notatek do użytkownika
- Ewidencja zdarzeń przypisanych do użytkowników
- Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory

Raporty

- Analiza aktywności użytkowników
- Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
- Analiza przerw w pracy
- Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
- Analiza aktywności mikrofonu oraz kamery

- Analiza wykorzystania poszczególnych aplikacji w czasie
- Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
- Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
- Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
- Statystyki najczęściej wykorzystywanych aplikacji
- Statystyki wykorzystania komputerów przez poszczególnych użytkowników
- Statystyki aktywności użytkownika i grup użytkowników
- Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin
- Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
- Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
- Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
- Monitoring wydruków na drukarkach sieciowych
- Monitoring użytkowników stacji terminalowych
- Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
- Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
- Raport zbiorczy historii zmian w rekordach użytkowników

Funkcje

- Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
- Autoryzacja nośników zewnętrznych

FORMULARZ PARAMETRÓW WYMAGANYCH

- Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
- Baza informacji o napędach zewnętrznych
- Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
- Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM
- Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy
- Informacje o ostatnio zalogowanych osobach na stacjach klienckich
- Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje
- Komentowanie przerw pracy
- Kategoryzacja przerwy w pracy na podstawie komentarza

Kontrola wykorzystania Internetu

Funkcje

- Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
- Blokada stron internetowych dla protokołu http \ https (IE, Chrome, Firefox, Opera, Edge, Chromium, Vivaldi)
- Kategoryzacja stron internetowych
- Blokada dostępu do witryn zgodnie z harmonogramem
- Blokada trybu incognito w przeglądarce Google Chrome

Raporty

- Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach
- Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
- Monitoring stron internetowych dla protokołu http \ https (IE, Edge, Chrome, Firefox, Opera, Vivaldi)
- Analiza liczby wejść na poszczególne strony lub domeny
- Analiza odwiedzanych domen i stron
- Raport informujący o plikach pobranych przez przeglądarki WWW
- Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe

Helpdesk

Obsługa

- Rejestracja i obsługa zgłoszeń
- Obsługa zgłoszeń w modelu Kanban
- Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
- Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
- Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
- Opis zgłoszenia w formacie HTML
- Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
- Tworzenie notatek dla zgłoszeń
- Zapisywanie wersji roboczej komentarza

FORMULARZ PARAMETRÓW WYMAGANYCH

- Archiwizacja zgłoszeń
- Monitoring czasu pracy nad incydentem (time tracking)
- Raport ewidencji czasu pracy nad zgłoszeniem
- Informacja o czasie reakcji do podjęcia zgłoszenia
- Dodanie prywatnego komentarza
- Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
- Dodanie załączników do incydentów, również do komentarza
- Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie
- Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
- Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
- Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
- Wydruk historii zgłoszenia
- Widok kalendarza (Planowanie rozwiązania incydentów)
- Korelacja incydentu z elementem zasobów
- Raport zbiorczy historii zmian
- Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
- Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
- Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu
- Określenie wpływu biznesowego wybranego zgłoszenia
- Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email

- Duplikacja i replikacja zgłoszeń

Konfiguracja

- Architektura drzewa dla kategorii zgłoszeń
- Tworzenie szablonów odpowiedzi
- Cykliczne raportowanie Listy incydentów
- Utworzenie własnych dodatkowych atrybutów dla zgłoszeń
- Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu
- Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)
- Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)
- Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
- Obsługa wielu kont pocztowych (Import + notyfikację email)
- Tworzenie własnych trybów oraz priorytetów incydentów
- Personalizacja widoku raportu listy incydentów
- Profile zgłaszających w helpdesk
- Personalizacja kolorów statusów zgłoszeń
- Automatyczne przypisywanie zgłoszeń do użytkowników

Moduł połączeń zdalnych

- Operacje na plikach i katalogach
- Zarządzanie procesami i rejestrem
- Monitoring pracy wykonywanej na komputerze
- Zdalny podgląd pulpitów wielu stacji (Funkcja Company Online)

FORMULARZ PARAMETRÓW WYMAGANYCH

- Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
- Wysyłanie wiadomości do użytkowników
- Uruchamianie na stacjach programów z wiersza poleceń Command Line
- Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
- Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego
- Przejęcie kontroli nad stacją roboczą
- Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
- Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
- Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
- Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
- Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
- Obsługa wielu monitorów dla podglądu pulpitu
- Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
- Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
- Połączenie pulpitem zdalnym w konfiguracji NAT-NAT
- Zarządzanie usługami systemu Windows
- Raport Sesje zdalnego pulpitu
- Wybór adresu IP, na którym ma być zestawione połączenie DirectPC
- Wybór portu, na którym klient nasłuchuje połączenia zdalnego

Baza wiedzy

- Wbudowana baza wiedzy
- Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk
- Edytor HTML

- Osadzanie załączników w treści artykułów
- Osadzanie multimediów w treści artykułów
- Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych
- Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk
- Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów
- Informacja o liczbie odsłon artykułu bazy wiedzy
- Bezpośrednie linkowanie artykułów bazy wiedzy

SLA

- Definiowanie planów umów SLA
- Definiowanie czasu obowiązywania umów SLA
- Definiowanie czasu pracy działów wsparcia technicznego
- Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych
- Definiowanie czasów reakcji oraz realizacji zgłoszenia
- Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji
- Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie
- Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA

Centralne repozytorium załączników

Funkcje

FORMULARZ PARAMETRÓW WYMAGANYCH

- Załączniki przechowywane w centralnym repozytorium
- Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu)
- Dodawanie i modyfikacja załączników z poziomu innych zasobów
- Załączniki typu: link, udział oraz plik
- Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura
- Historia zmian załącznika

Zarządzanie użytkownikami

Funkcje

- Raportowanie aktywności pracy
- Przeglądanie ostatnio zgłoszonych incydentów
- Powiązanie użytkownika z licencją
- Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
- Cykliczne, automatyczne generowanie raportów
- Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
- Zgłoszenia dotyczące wniosków nieobecności użytkowników
- Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności
- Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
- Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
- Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO
- Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
- Planowanie dni wolnych w widoku kalendarza
- Planowanie zastępstw podczas nieobecności

Raportowanie cykliczne

Użytkownicy

- Raport historia sesji
- Raport Nośniki danych
- Raport Operacje na plikach
- Raport wydruków
- Raport użycia aplikacji
- Raport odwiedzonych stron WWW
- Raport Wysyłane pliki
- Raport czasu pracy przy komputerze
- Raport Bizlook

Zasoby

- Raport historii zasobów
- Raport informujący o nowych zasobach
- Raport informujący o nadchodzących terminach w zasobach

FORMULARZ PARAMETRÓW WYMAGANYCH

- Raport Zasoby zarchiwizowane

Podstawowe

- Raport Informacje o autoryzowanych agentach

Oprogramowanie

- Raport zainstalowanego oprogramowania
- Raport Szczegóły plików

Helpdesk

Raport incydentów (Helpdesk)

Raport czasu pracy nad zgłoszeniem

Raport Czasy SLA

Automatyzacja

Lista dostępnych reguł

- Zakończenie asysty serwisowej AS lub AS Plus
- Wygaśnięcie certyfikatu SSL
- Kończące się licencje na agenta

- Zapełniona baza danych

Zasoby

- Brak połączenia od agenta
- Brak wolnej przestrzeni na dysku
- Ostrzeżenie od Windows Security Center
- Zakończenie skanowania sprzętu
- Dodanie zasobu
- Zmiana zasobu
- Usunięcie zasobu
- Zakończenie okresu gwarancyjnego
- Zakończenie umowy serwisowej

Oprogramowanie

- Zmiana oprogramowania
- Zakończenie skanowania oprogramowania
- Zamknięcie audytu

Licencje

- Dodanie licencji
- Zmiana licencji

FORMULARZ PARAMETRÓW WYMAGANYCH

- Usunięcie licencji
- Wygaśnięcie licencji
- Planowana wymiana licencji

Użytkownicy

- Dodanie użytkownika
- Zmiana użytkownika
- Usunięcie użytkownika

Helpdesk

- Dodanie zgłoszenia
- Usunięcie zgłoszenia
- Zmiana zgłoszenia

Lista dostępnych Akcji

- Wykonywanie skryptu na podstawie zdefiniowanej reguły
- Wysłanie powiadomienia w konsoli na podstawie zdefiniowanej reguły
- Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły
- Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły

RODO

Funkcje

- Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie
- Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie
- Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia
- Wstępne wypełnienie wniosków o zmianę dostępu
- Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
- Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
- Archiwizacja zbiorów
- Definiowanie czynności przetwarzania
- Przypisywanie zbioru danych do czynności przetwarzania
- Przydzielanie dostępów do czynności przetwarzania
- Zapisywanie historii zmian wniosków o dostęp do zbiorów

Raporty

- Raport zbiorczy Czynności przetwarzania
- Raport zbiorczy Zbiory danych
- Raport zbiorczy zinwentaryzowanych dostępów
- Raport zbiorczy zinwentaryzowanych powierzeń
- Raport zbiorczy zinwentaryzowanych dokumentów
- Raport zbiorczy historii naruszeń bezpieczeństwa
- Raport zbiorczy wniosków o dostęp

FORMULARZ PARAMETRÓW WYMAGANYCH

Sygnalista

Funkcje

- Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej
- Usuwanie metadanych z załączników zgłoszeń
- Usuwanie danych osobowych ze zgłoszeń
- Podział interfejsu na publiczny oraz dla wewnętrzny
- Dashboard podsumowujący wykorzystanie portalu sygnalisty
- Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła
- Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka
- Definiowanie stron publicznych (dostępnych dla sygnalistów)
- Obsługa wielu języków stron publicznych

Raporty

- Raport zgłoszeń
- Historia zmian
- Statystyka zgłoszeń
- Pozostały czas na przyjęcie zgłoszenia
- Pozostały czas do zakończenia
- Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane

Portal Web

Funkcje

- Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów
- Rozbudowane filtry dla raportów tabelarycznych
- Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami
- Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji
- Raporty dla każdego modułu w formie tabelarycznej
- Obsługa helpdesk oraz bazy wiedzy
- Obsługa modułu RODO
- Obsługa modułu automatyzacja
- Automatyczne logowanie przy pomocy aplikacji
- Logowanie za pomocą poświadczeń domenowych (SSO)
- Wydruk raportów tabelarycznych
- Kontrola statystyk użytkowników
- Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)
- Przełączanie wersji językowej bez ponownego logowania do systemu Nawigacja Breadcrumb

Funkcjonalności ogólne

- Określanie praw dostępu do grup zasobów lub użytkowników
- Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na

FORMULARZ PARAMETRÓW WYMAGANYCH

dowolnej liczbie komputerów ("Licencja pływająca")
- Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
- Wersja angielska (en-US) interfejsu użytkownika
- Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
- Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
- Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
- Odczytywanie struktury organizacji z Active Directory
- Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
- Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
- Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
- Definiowanie nieograniczonej liczby użytkowników systemu
- Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy
- Indywidualny login i hasło dla poszczególnych użytkowników
- Automatyczne logowanie do systemu
- Zarządzanie uprawnieniami użytkowników - możliwość ograniczenia dostępu do poszczególnych funkcji programu
- Określanie ról użytkowników - zarządzanie grupami
- Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
- Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
- Zgodny z pracą w sieciach WLAN
- Podgląd aktualnych zadań serwera
- Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
- Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami

- Wyszukiwanie danych w tabelach raportów Dowolne definiowania grup sprzętu i użytkowników
- Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
- Definiowanie i zapamiętywanie własnych widoków Eksport danych bezpośrednio do MS Excel Budowa zestawień metodą drag'n'drop
- Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
- Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
- Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
- Mechanizm kompresji pakietów danych przesyłanych przez Agenta
- Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
- Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
- Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
- Mechanizm zdalnego pobierania bieżących aktualizacji do programu
- Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
- Dostęp do bazy wiedzy systemu
- Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
- Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia bckupu bazy w trybie wsadowym

FORMULARZ PARAMETRÓW WYMAGANYCH

- Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
- Personalizacja pakietu instalacyjnego agenta
- Określanie polityki haseł dla systemu
- Zmiana języka systemu podczas logowania
- Określenie numeru BDO przy definiowaniu rekordu firmy
- Opcja resetu hasła podczas logowania
- Globalne wyszukiwanie obiektów w systemie
- Utworzenie atrybutów jako lista/słownik
- Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
- Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring Wyszukiwarka ustawień w opcjach systemowych
- Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
- Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
- Skanowanie lasu domen
- Automatyczne zamknięcie oferowanego systemu po zakończeniu sesji
- Logowanie do portalu Web za pomocą mechanizmu Single Sign On
- Logowanie operacji kont serwisowych

Dodatkowe informacje

- Wersja darmowa z ograniczeniem do 3 agentów oraz 3 użytkowników
- Kreator instalacyjny ułatwiający wdrożenie systemu
- Aplikacja Master\Server\ Agent w wersji x86\x64
- Rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
- Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019 32/64 bit)
- Praca w oparciu o PostgreSQL 9.6 lub nowszy
- Obsługa systemów operacyjnych - Agent: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
- Obsługa systemów operacyjnych - Master : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
- Obsługa systemów operacyjnych - Serwer: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
- Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem Symantec SHA256 TimeStamping Signer - G2
- Sterowniki systemowe są podpisane certyfikatem GlobalSign Extended Validation CodeSigning CA - SHA256 - G3 i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.

Licencje

- Licencja dla administratora systemu – min 2.
- Licencje dla użytkowników końcowych – min 70.

9/TP/2022 Załącznik nr 5 do SWZ

FORMULARZ PARAMETRÓW WYMAGANYCH

UWAGA, Zamawiajacy informuje, że w każdej sytuacji kiedy odnosi się do konkretnych norm, dopuszcza wszystkie inne normy równoważne.

Oświadczamy, że zaoferowany przedmiot zamówienia jest zgodny ze wszystkimi wymaganiami przedstawionymi niniejszym w formularzu . ……. data i podpis Wykonawcy