Opis przedmiotu zamówienia

# Cz. I: Zakup oprogramowania do gromadzenia i analizy logów

* 1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
  2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.
  3. Wykonawca jest zobowiązany dostarczyć urządzenie typu NAS do gromadzenia logów o następujących parametrach:

|  |  |
| --- | --- |
| Procesor | Jeden 4-rdzeniowy/8-wątkowy procesor AMD Ryzen V1500B lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4500 pkt.  W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie <https://www.cpubenchmark.net> na dzień ogłoszenia przetargu lub nowszy. |
| Obudowa | Tower o wymiarach max. 167 × 200 × 224 mm |
| Pamięć RAM | 8 GB pamięci SO-DIMM DDR4 ECC |
| Ilość obsługiwanych dysków | 4 dysków o maksymalnej pojemności 24 TB każdy  2 dyski M.2 NVMe 2280 |
| Ilość zainstalowanych dysków | 4 dyski HDD klasy Plus w formacie 3,5” znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 12 TB;  Możliwość aktualizacji oprogramowania dysków z poziomu NAS. |
| Interfejsy sieciowe | 2 x 2,5Gb |
| Porty | 2 x USB 3.2 Gen 1, 1x port rozszerzenia USB Typ-C |
| Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10 |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, SNMP, VPN |
| Usługi | Serwer VPN  Serwer pocztowy dla kilku domen  Stacja monitoringu  Windows ACL  Integracja z Windows ADS  Firewall  Serwer WWW  Serwer plików  Manager plików przez WWW  Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie  Usługa DDNS  Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID  Snapshot Replication  Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware  Wsparcie dla High Availability |
| Obsługa migawek | • Maksymalna liczba migawek folderów współdzielonych: 256  • Maksymalna liczba migawek systemu: 2048 |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów |
| Język GUI | Polski |
| Certyfikaty | CE |
| System plików | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT32, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego |
| Liczba wolumenów | Do 32 |
| Liczba iSCSI Targetów | Do 32 |
| Liczba iSCSI LUN | Do 64 |
| Liczba kont użytkowników | 512 |
| Liczba grup | 128 |
| Liczba folderów udostępnionych | 128 |
| Zasilacz | 100W |
| Chłodzenie | FAN x 2 92 mm x 92 mm |
| Gwarancja i serwis | 3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie  3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na dyski |

1. Wymagania techniczne dotyczące rozwiązania
   1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
   2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na wirtualnej maszynie w środowisku Hyper-V.
   3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
   4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną o następujących parametrach:
      * Procesor (CPU): 8 rdzeni,
      * Pamięć RAM: 16 GB,
      * Dysk twardy (HDD): 2 TB.
   5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
   6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
   7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
   8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
   9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
   10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.
2. Wdrożenie systemu
   1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
   2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
   3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego maszynie wirtualnej.
   4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspójniające zegary czasów w sieci Zamawiającego.
   5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
   6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
   7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
      * 3 urządzenie klasy UTM firmy Fortinet,
      * 10 przełączniki zarządzalne firmy Mikrotik,
      * 8 serwery Windows,
      * 3 serwery Linux,
      * 85 stacji roboczych Windows 10 i 11,
      * 1 aplikację centralnego zarządzania ESET Endpoint Security,
      * 4 serwery wirtualizacji Hyper-V,
   8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
   9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
   10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
   11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
   12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
   13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
   14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

# Cz. II: Zakup systemu klasy DLP

1. System operacyjny: a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi c. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych
31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia.
39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.
40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.
41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.
42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.
43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.
44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.
45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.
46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf.

# Cz. III: Zakup systemu do monitoringu sieci

|  |
| --- |
| **Zarządzanie zasobami** |
| **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 interfejsów sieciowych oraz 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, EntraID oraz Intune(Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) |
| Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci |
| 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 |
| 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 |
| Dowolna treść kodu kreskowego |
| Określanie loga firmy oraz użycia go na wydrukach |
| Grupowa zmiana domeny/grupy roboczej zasobu |
|  |
| **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 |
| 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 |
| Określanie ikony dla typów zasobów |
| Integracja z Dell API |
| Wyszukiwanie i identyfikacja duplikatów zasobów |
| Geolokalizacja komputerów z agentem |
|  |
| **Raporty zasobów** |
|  |
| Raport dodanych załączników |
| Automatyczne tworzenie historii zmian sprzętu |
| Raport zbiorczy historii zmian w sprzęcie |
| Ewidencja zdarzeń serwisowych |
| Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów |
| Informacja na temat pojemności dysków twardych oraz wolnego miejsca |
| Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu |
| Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu |
| Kreator szablonów wydruków WYSIWYG |
| Definiowanie dedykowanych profili protokołów |
| Generowanie protokołów szyfrowania komputerów / telefonów |
| Zapisywanie protokołów podczas generowania jako załącznik do zasobu |
| Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia |
| Wydruk lub zapis do pliku raportów ze szczegółami sprzętu |
| Porównywarka wyników skanowania sprzętu |
| Dzienniki zdarzeń systemu Windows |
| Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu |
| Geolokalizacja komputerów z agentem |
|  |
| **Zarządzanie zasilaniem** |
|  |
| Zdalne włączanie i wyłączenie komputerów |
| Obsługa SecureOn przy WakeOnLan |
| Tworzenie harmonogramów wyłączania i włączania komputerów |
| Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart |
| Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik |
| Możliwość przerwania / odłożenia zadania na żądanie użytkownika |
| Wymuszenie wylogowania użytkownika przed wyłączeniem komputera |
| Raport zadań jednorazowych oraz harmonogramów |
| Monitoring obciążenia CPU |
|  |
| **Funkcje dodatkowe** |
|  |
| Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych |
| Generowanie skryptów z wykorzystaniem AI |
| Podpisywanie skryptów Powershell certyfikatem |
| Wykonywanie skryptów w kontekście sesji użytkownika lub usługi |
| Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika |
| Wykonywanie zadań dla wszystkich komputerów |
| Edytor skryptów z funkcją kolorowania składni |
| Wykorzystywanie predefiniowanych skryptów |
| 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) |
| 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 |
| 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 |
| Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego |
| Import licencji z pliku tekstowego |
| Automatyczne generowanie historii zmian w licencji |
| Określanie statusu licencji |
| Tworzenie 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.) |
| 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 |
| Odczyt skrótów MD5 MD5, SHA-1, SHA256, SHA384, SHA512 plików |
| 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 oprogramowania** |
|  |
| 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 |
| Automatyczna klasyfikacja używanych programów z wykorzystaniem AI |
| 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) |
| Zdalna 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 kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach |
| Odczyt informacji o kontal lokalnych komputera, wraz z odczytem grup do, których konto należy |
| 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). |
| 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 oraz AAD |
| Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD) |
| 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 |
| Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko |
| 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 na podstawie wykrytych urządzeń |
| Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych |
| Automatycznie budowana baza informacji o napędach zewnętrznych |
| Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.) |
| Odczyt i blokada urządzeń PTP/MTP |
| 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 pobierania plików wg typu MIM |
| Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW |
| Kategoryzacja stron internetowych |
| Import stron WWW z pliku lub ze schowka |
| Slowniki kategorii stron WWW |
| Blokada dostępu do witryn zgodnie z harmonogramem |
| Blokada dostępu do witryn na podstawie kategorii strony WWW |
| Blokada trybu incognito w przeglądarce Google Chrome |
|  |
| **Raporty** |
| Raporty dotyczące aktywności użytkowników w Internecie |
| Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki ) |
| Monitoring stron internetowych dlaprotokołu http \ https (Przeglądarki oparte o silnik Chromium, Edge, Chrome, Vivaldi, Firefox\*) |
| Analiza liczby wejść na poszczególne strony lub domeny |
| Kategoryzacja odwiedzanych domen i stron, opcjonalnie z wykorzystaniem AI |
| Raport informujący o plikach pobranych przez przeglądarki WWW |
| Raport informujący o danych wysłanych przez przeglądarki (bez Firefox) |
| Monitoring plików pobieranych przez przeglądarki internetowe |
|  |
| **Helpdesk** |
| **Obsługa** |
|  |
| Rejestracja i obsługa zgłoszeń |
| Obsługa zgłoszeń w modelu Kanban |
| Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny) |
| Edycja zgłoszeń powiązanych w oknie zgłsozenia bieżącego |
| 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 |
| 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 |
| Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA |
| 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 |
| Powiadomienia o liczbie nieprzeczytanych zgłoszeń |
| Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł |
| Asystent AI do generowania odpowiedzi, podsumowania zgłoszenia, tłumaczeń, generowania tagów oraz wykrywania kategorii zgłoszeń |
|  |
| **Konfiguracja** |
|  |
| Architektura drzewa dla kategorii zgłoszeń |
| Tworzenie szablonów odpowiedzi |
| Cykliczne raportowanie Listy incydentów |
| Tworzenie własnych dodatkowych atrybutów dla zgłoszeń |
| Tworzenie i zarządzanie typami statusów zgłoszeń |
| Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika |
| 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 |
| Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego |
| Konfiguracja maksymalnej wielkości załącznika |
|  |
| **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) |
| 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 full-screen |
| 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 |
| Wykorzystanie autorskiego protokołu lub MS RDP do połączeń zdalnych |
| Obsługa wiersza poleceń / Powershell w trybie live |
|  |
| **Baza wiedzy** |
|  |
| Wbudowana baza wiedzy |
| Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk |
| Kopiowanie artykułów |
| Edytor HTML |
| Osadzanie załączników w treści artykułów |
| Osadzanie multimediów w treści artykułów |
| Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych |
| Szybkie kopiowanie wpisów bazy wiedzy |
| 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** |
|  |
| 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 |
| Blokowanie kont Windows |
|  |

|  |
| --- |
| **Raportowanie cykliczne** |
| **Raporty automatyczne, wysyłane zgodnie z określonym harmonogramem oraz listą odbiorców.** |
| **Użytkownicy** |
|  |
| Raport historia sesji |
| Raport Nośniki danych |
| Raport Operacje na plikach |
| Raport wydruków |
| Raport użycia aplikacji |
| Raport nagłówów okien |
| Raport odwiedzonych stron WWW |
| Najczięściej odwiedzane strony internetowe |
| 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 |
| Raport Zasoby zarchiwizowane |
| Raport Systemy Operacyjne |
|  |
| **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 |
| Czasy SLA |
| Czas realizacji |
|  |
| **Automatyzacja** |
| **Lista dostępnych reguł** |
| Akcje (modyfikacje obiektów systemu, skrypty, powiadomienia mail / SMS / popup) wykonywane w przypadku wystąpienia wybranych wyzwalaczy. |
| **Ogólne** |
|  |
| Zakończenie asysty serwisowej AS lub AS Plus |
| Wygaśnięcie certyfikatu SSL |
| Kończące się licencje na agenta |
| Zapełniona baza danych |
| Dziennik operacji (uruchamiana po dodaniu wpisów do dziennika operacji) |
| Zbyt duży rozmiar folderu cache |
|  |
| **Zasoby** |
|  |
| Brak połączenia agenta |
| Brak wolnej przestrzeni na dysku |
| Ostrzeżenie od Windows Security Center |
| Zakończenie skanowania sprzętu |
| Powielenie agenta |
| Podłączenie dysku zewnętrznego |
| Stan modułu TPM |
| Stan szyfrowania woluminów |
| Dodanie zasobu |
| Zmiana zasobu |
| Usunięcie zasobu |
| Zakończenie okresu gwarancyjnego |
| Zakończenie umowy serwisowej |
| Powielenie zasobów |
| Nowy wpis w dzienniku zdarzeń Windows |
|  |
| **Oprogramowanie** |
|  |
| Zmiana oprogramowania |
| Zakończenie skanowania oprogramowania |
| Zakończenie okresu wsparcia technicznego |
| Zamknięcie audytu |
|  |
| **Licencje** |
|  |
| Dodanie licencji |
| Zmiana licencji |
| Usunięcie licencji |
| Wygaśnięcie licencji |
| Planowana wymiana licencji |
|  |
|  |
| **Użytkownicy** |
|  |
| Dodanie użytkownika |
| Zmiana użytkownika |
| Usunięcie użytkownika |
| Logowanie użytkownika |
| Wylogowanie użytkownika |
| Strony WWW |
| Nagłówki okien |
|  |
| **Helpdesk** |
|  |
| Dodanie zgłoszenia |
| Usunięcie zgłoszenia |
| Zmiana zgłoszenia |
| Zapisana wersja robocza |
| Brak aktywności w zgłoszeniu |
|  |
| **Lista dostępnych Akcji** |
|  |
| Wykonywanie skryptu na podstawie zdefiniowanej reguły |
| Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci) |
| Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły |
| Dodanie komentarza (dla reguł Helpdesk) |
| Wysyłka wiadomości SMS |
| Wysylka powiadomień MS Teams |
| Przypisz atrybut |
|  |

|  |
| --- |
| **RODO** |
| **Funkcje** |
|  |
| Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie |
| Filtrowanie zbiorów danych oraz czynności przetwarzania |
| 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 |
| Dodawanie historycznych dostępów oraz wniosków o dostęp |
| Filtrowanie użytkowników w raporcie Dostępy |
|  |
| **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 |
| Raport zbiorczy Dostępy |
|  |
| **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 |
| Natywne wsparcie języka ukraińskiego |
| Definiowany limit załączników |
| Wyróżnienie zgłoszeń o przekroczonym czasie reakcji |
| Blokowanie załączników do zgłoszeń |
| Pełna obsługa panelu sygnalisty za pomocą klawiatury |
| Integracja OPSWAT Metadefender dla wersji Core i Cloud |
| Skanowanie załączników programem antywirusowym |
| Własne opisy pól formularza sygnalisty |
| Obsługa zgód i akceptacji |
| Dostosowanie widoku sygnalisty do WCAG2.2 |
|  |
| **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** |
|  |
| Personalizacja portalu (logo, kolorystyka) |
| Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu |
| Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów |
| Widok “Mój dzień” zawierający oś czasu z aktywnością użytkownika |
| 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 |
| Obsługa modułu Sygnalita |
| Automatyczne logowanie przy pomocy aplikacji |
| Logowanie za pomocą poświadczeń domenowych (SSO) |
| Logowanie za pomocą konta AzureAD lub AAD |
| 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 |
| Definicja własnego URL, bez zmiany nazwy hosta (obsługa loadbalancingu) |
|  |
| **Funkcjonalności ogólne** |
|  |
|  |
| Określanie praw dostępu do grup zasobów lub użytkowników |
| Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca") |
| Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem |
| Obsługa systemu w wielu zakładkach (też w aplikacji desktop) |
| Wersja polska (pl-PL) interfejsu użytkownika |
| Praca w oparciu o silnik bazy danych MS SQL |
| Zdalna instalacja i dezinstalacja agentów na stacjach roboczych |
| Odczytywanie struktury organizacji z Active Directory |
| Skaner sieci wykorzystywany do wykrywania nowych urządzeń |
| 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,Pracownicy |
| Indywidualny login i hasło dla poszczególnych użytkowników |
| Automatyczne logowanie do systemu |
| Zarządzanie uprawnieniami użytkowników - okreśłanie dostępu do poszczególnych obiektów i opcji systemu systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie) |
| Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego |
| 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). Uruchomienie narzędzia backupu bazy w trybie wsadowym |
| Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania, sprzętu, sesji zdalnego pulpitu, logów raportów, logów automatyzacji |
| Harmonogram konserwacji - planowanie godzin oczyszczania bazy |
| 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 |
| Tworzenie 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 |
| Budowa personalizowanego pakietu instalacyjnego |
| Logowanie do portalu Web za pomocą mechanizmu Single Sign On |
| Logowanie operacji kont serwisowych |
| Logowanie nieudanych prób uwierzytelnienia |
| Eksport danych diagnostycznych oraz dzienników operacji |
| Integracja z SMS API |
| Definiowanie nazwy hosta, na której serwer nasłuchuje połączeń sieciowych |
| Integracja z OpenAI (asystent systemu) |
|  |

|  |
| --- |
| **Dodatkowe informacje** |
|  |
|  |
| Wersja darmowa z ograniczeniem do 3 agentów oraz 3 użytkowników |
| Kreator instalacyjny ułatwiający wdrożenie systemu |
| Aplikacja Master\Server\ Agent w wersji 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 lub nowszymi 32/64 bit) |
| Obsługa systemów operacyjnych - **Agent**: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, 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 Server 2022, 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 Server 2022, Windows 7, Windows 8, Windows 10, Windows 11, Linux (w trybie preview) |
|  |
| Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem ***DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)*** |
| Sterowniki systemowe są podpisane certyfikatem ***Extended Validation (EV) Code Signing Certificate*** (***GlobalSign***) i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™. |
|  |

USŁUGA ASYSTY WDROŻENIOWEJ SYSTEMU STATLOOK

* 1. 1. Usługa Asysty Wdrożenia obejmuje: a. instalację oprogramowania: Serwer, Master, Agent na max. 10 stacjach roboczych,
     + 1. b. szkolenie administratora z zakresu pracy z programem,
  2. c. przykładowy audyt oprogramowania na wybranej stacji roboczej.
  3. d. Asysta może być przeprowadzana zdalnie, przy użyciu narzędzi do zdalnej pomocy

# Cz. IV: Zakup przełączników sieciowych

1. **Przełącznik sieciowy typ 1 – 9 szt. o następujących parametrach:**

|  |  |
| --- | --- |
| **Typ obudowy** | Rack |
| **Porty RJ-45 1Gb/s** | Min. 24 |
| **Porty SFP+ 10 Gb/s** | Min. 4 |
| **Procesor** | Min. jedno rdzeniowy, taktowany min. 800 MHz |
| **Pamięć RAM** | Min. 512 MB |
| **Pamięć wewnętrzna** | Min. 16 MB flash |
| **Oprogramowanie** | Preinstalowany system operacyjny o następujących funkcjonalnościach:  - firewall (filtrowanie adresów IP, protokołów IP, DSCP)  - obsługa IPv6  - routing statyczny  - wirtualny routing (VRF)  - protokoły routingu dynamicznego (OSPF v2, BGP v4)  - obsługa VPN  - DHCP server  - wsparcie RADIUS  - HTTP caching proxy server |
| **Zakres temperatury pracy** | Min. Od -20 do 60 stopni Celsjusza |
| **Zasilanie** | Pojedynczy zasilacz |
| **Chłodzenie** | Aktywne, min. 2 wentylatory |
| **Wymiary** | Max. 444 x 301 x 45 mm |
| **Akcesoria w zestawie** | Kabel zasilający, zestaw montażowy w szafie rack |
| **Certyfikaty** | CE, EAC, ROHS |
| **Gwarancja** | Min. 1 rok gwarancji door-to-door producenta lub autoryzowanego partnera producenta |

1. **Przełącznik sieciowy typ 2 – 1 szt. o następujących parametrach:**

|  |  |
| --- | --- |
| **Typ obudowy** | Rack |
| **Porty SFP+ 10 Gb/s** | Min. 16 |
| **Procesor** | Min. dwu-rdzeniowy, taktowany min. 800 MHz |
| **Pamięć RAM** | Min. 1 GB |
| **Pamięć wewnętrzna** | Min. 16 MB flash |
| **Oprogramowanie** | Preinstalowany system operacyjny o następujących funkcjonalnościach:  - firewall (filtrowanie adresów IP, protokołów IP, DSCP)  - obsługa IPv6  - routing statyczny  - wirtualny routing (VRF)  - protokoły routingu dynamicznego (OSPF v2, BGP v4)  - obsługa VPN  - DHCP server  - wsparcie RADIUS  - HTTP caching proxy server |
| **Zakres temperatury pracy** | Min. Od -20 do 60 stopni Celsjusza |
| **Zasilanie** | Redundantne zasilacze |
| **Chłodzenie** | Aktywne, min. 2 wentylatory |
| **Wymiary** | Max. 444 x 225 x 45 mm |
| **Akcesoria w zestawie** | Kabel zasilający, zestaw montażowy w szafie rack |
| **Certyfikaty** | CE, EAC, ROHS |
| **Gwarancja** | Min. 1 rok gwarancji door-to-door producenta lub autoryzowanego partnera producenta |

# Cz. V: Zakup zasilaczy awaryjnych UPS

**Zasilacz awaryjny – 50 szt. o następujących parametrach:**

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| moc pozorna | min. 1200 VA |
| moc rzeczywista | min. 600 W |
| Technologia | VI (line interactive) |
| Typ obudowy | Tower |
| **praca sieciowa** |  |
| Napięcie wejściowe | 170 ÷ 280 V AC ± 7 % |
| Częstotliwość napięcia wejściowego | 45 ÷ 55 Hz ± 1 Hz |
| Zakres napięcia wyjściowego | 230 V AC |
| Kształt napięcia wyjściowego | Schodkowa aproksymacja sinusoidy / Tak jak na wejściu |
| Progi przełączania sieć – UPS | 170 ÷ 280 V AC ± 7 % |
| Czas przełączania sieć – UPS | <6ms |
| **praca bateryjna** |  |
| Napięcie wyjściowe | ~230V ± 10% |
| Częstotliwość napięcia wyjściowego | 50Hz |
| Kształt napięcia wyjściowego na pracy bateryjnej | Schodkowa aproksymacja sinusoidy |
| Progi przełączania UPS – sieć | 176 V ÷ 274 V AC ± 7 % |
| Zabezpieczenie wyjściowe przeciwzwarciowe | elektroniczne |
| Zabezpieczenie wyjściowe przeciążeniowe | elektroniczne |
| Czas podtrzymania (P 0,8max/P 0,5max) | minimum 4.5 / 11 min |
| akumulatory wewnętrzne | Minimum 2 x 12V 7Ah; szczelne, bezobsługowe |
| **pozostałe** |  |
| wejście zasilania | Minimum 1 x IEC C320 C14 |
| Ilość i typ gniazd wyjściowych | Minimum 2 x IEC C320 C13 (10A), 2 x PN-E-93201 |
| Filtr telekomunikacyjny | minimum filtr teleinformatyczny RJ-45 |
| Sygnalizacja | Akustyczno-optyczna |
| Wyświetlacz LCD | wymagany - sygnalizujący minimum 4 stopniową skalę poziomu obciążenia oraz 4 stopniową skalę naładowania baterii. Pokazujący napięcie wejściowe i wyjściowe oraz sygnalizujący aktywność systemu AVR. Sygnalizujący usterkę inną niż przeciążenie lub zwarcie. |
| Zimny Start | tak |
| Interfejs komunikacyjny | USB (kabel w komplecie) |
| Waga UPS | do 9 kg |
| wymiary | nie większe niż: wysokość 196 mm; szerokość 140 mm; głębokość 366 mm |
| gwarancja | min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; |
| serwis |  |
| serwis realizowany w systemie door-to-door |
| oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS . |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |
| możliwość edycji nazw urządzeń na liście monitorowanych UPSów |
| wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| certyfikaty producenta (załączyć do oferty) | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; |
|  | deklaracja CE producenta sprzętu |